Adobe Acrobat Sign Solutions

Acrobat Sign Solutions & Healthcare and Life Science Organizations: A Handbook for 21 CFR Part 11 and EudraLex Annex 11

April 2025

Adobe

Contents

1 Introduction

1 Introduction

Acrobat Sign Solutions is a flexible and trusted cloud-based electronic signature service that enables organizations to manage their signing workflows — from the simplest standard signature to a highly secure certificate-based digital signature.

Today, many organizations operating under the United States (U.S.) Food and Drug Administration (FDA) oversight (such as food, drug, biologics, medical devices, cosmetics, and veterinary product companies) are choosing Acrobat Sign Solutions to implement automated electronic signature workflows in place of traditional paper-and-ink signature processes. The U.S. FDA enforces the 21 CFR Part 11 regulation to ensure that systems used to create, modify, maintain, or transmit electronic records are designed to safeguard the authenticity and integrity of the electronic records (including the electronic signatures applied to those records).

In the European Union (EU), EudraLex is the collection of rules and regulations governing medicinal products for human and veterinary use. Under EudraLex rules, Volume 4 Annex 11 establishes the conventions for using computerized systems.

For Healthcare and Life Science organizations operating under GxP regulations, being able to use Acrobat Sign Solutions in a manner that complies with 21 CFR Part 11 and/or EudraLex Annex 11 requirements is essential.

This handbook discusses how, with proper system implementation and appropriate procedural controls, electronic signatures generated through Acrobat Sign Solutions can be enforceable and help organizations comply with their requirements under 21 CFR Part 11 and EudraLex Annex 11. This handbook describes key features available in Acrobat Sign Solutions along with typical use cases to illustrate how these features can be implemented to help organizations meet the requirements of 21 CFR Part 11 and EudraLex Annex 11. In addition to describing features, this handbook also covers the quality management processes implemented by Adobe that support the seamless adoption and continued use of Acrobat Sign Solutions.

2 Scope

2 Scope

This handbook provides information, guidance, and recommendations for the implementation and use of Acrobat Sign Solutions in a manner that helps organizations meet 21 CFR Part 11 and EudraLex Annex 11 requirements. The intended reader of this paper is the Healthcare and Life Science organization using Acrobat Sign Solutions as part of a GxP regulated process ("Customer").

This handbook focuses on standardized scenarios for the application of electronic signatures to controlled GxP documents through the Acrobat Sign service as provided in **Adobe Acrobat Sign Solutions,** enterprise or business levels of service.

Acrobat Sign features provided in Acrobat Pro, Acrobat Standard, and Acrobat Reader are not considered within this handbook.

This handbook covers the Acrobat Sign features provided in the web application only. The use of the Adobe Acrobat Sign mobile app on a tablet or mobile phone is not discussed in this document.

This handbook does not cover electronic signatures generated with Adobe Acrobat and Reader desktop, using APIs to connect systems to Acrobat Sign Solutions, or other applications. Prior to proceeding with such implementations, further assessment shall be carried out by the Customer to determine suitability and compliance capability.

While Acrobat Sign Solutions offer various features to facilitate the digitization of business processes, the use of functionality that supports the use of templates, custom workflows, and APIs is specific to each Customer's implementation. As such, these types of features are not discussed in this document.

Healthcare and Life Science organizations that are concerned with protecting Protected Health Information (PHI) in compliance with HIPAA can implement privacy and added security safeguards within Acrobat Sign Solutions. However, compliance with HIPAA is not explicitly addressed within this handbook.

This handbook focuses on the Acrobat Sign service as provided in the commercial instance of Acrobat Sign Solutions. Adobe Acrobat Sign for Government is a separate instance whose environment is engineered to be FedRAMP Moderate compliant. However, Adobe Acrobat Sign for Government and compliance with FedRAMP security requirements are not addressed in this document.

While the information in this handbook is intended to help organizations understand the functionalities of Acrobat Sign Solutions that meet the requirements of 21 CFR Part 11 and EudraLex Annex 11, organizations should rely on their own legal counsel when planning a compliant deployment of Acrobat Sign Solutions.

3 Glossary of Terms

3.1 General Terms

Adobe Admin Console	An administrative portal used by enterprises to manage users and licenses across all Adobe products and services.
Agreement	Term used to define both the object created from file(s) uploaded into the Acrobat Sign service during the process of obtaining signatures and the final PDF that is generated.
Customer	Any organization that subscribes to an Acrobat Sign Solutions account with the intention (in the case of this handbook) to use Acrobat Sign as part of a process that must be compliant with 21 CFR Part 11 and/or EudraLex Annex 11 requirements.
Customer Account (or Acrobat Sign Account)	A specific instance of Acrobat Sign Solutions belonging to a Customer.
User	Any person who is identified by a unique email address and who uses Acrobat Sign Solutions in the capacity of *Signer, Sender, or Administrator (Account, Group)*. A user is described as Internal or External as follows: An **Internal user** is any individual who is an active member of the Customer Account from which an agreement was sent. An **External user** is any individual who is not a member of the Customer Account from which the agreement was sent.
User Account	Information about the user (such as email address and password) that allows for the individuals who have been added to a Customer Account to authenticate to the system.

3.2 Groups, Roles, and Privileges

Admin Console Administrator	An Adobe Admin Console user with the authority to manage users and licenses across all Adobe products and services purchased by the organization. An Admin Console Administrator does not need to be an Acrobat Sign Solutions user.
Account Administrator	An Acrobat Sign Solutions user with elevated permissions to define account settings, to create groups, and may be responsible for adding and/or administering users. Account Administrators must be members of the Customer Account. An Account Administrator does not need to be an Admin Console Administrator.
Group	An entity within the Customer Account to which distinct configuration settings may be applied. Internal users are assigned to one or more groups.
Group Administrator	An Acrobat Sign Solutions user with limited administration capabilities to define group settings and may be responsible for administering users assigned to that group. Group Administrators must be members of the Customer Account. A user can be designated as Group Administrator of one or more groups.
Sender	An Acrobat Sign Solutions user with appropriate permissions to send documents to Signers for the application of electronic signatures. To route a document for signature, the Sender uploads the document in the Send page interface within Acrobat Sign Solutions and specifies email addresses for the Signers (recipients). Senders must be members of the Customer Account.
Signer (or Recipient)	An individual who receives a request to apply an electronic signature to a document in Acrobat Sign Solutions. The Signer receives an email containing a hyperlink or instructions to access the document, informing them that the document is awaiting signature. Signers can access and sign documents from any device through a secure web browser session. Signers can be people inside or outside the Customer Account (i.e. a Signer does not necessarily need to have a user account). For the purposes of this document, we will refer to them as Internal or External described as follows: • An **Internal Signer** is any individual (identified by their email address) who is an active user within the same Customer Account from which the agreement was sent and who is the recipient of a request to apply an electronic signature to a document. Internal Recipient may be used interchangeably with Internal Signer. **Self-signing** is also possible when an Internal Signer has an agreement that they need to sign alone. • An **External Signer** is any individual who is not a member of the Customer Account from which the agreement was sent and who is the recipient of a request in Acrobat Sign Solutions to apply an electronic signature to a document. External Recipient may be used interchangeably with External Signer. Although External Signers do not need to have an Acrobat Sign user account to be able to sign an agreement, they can be a member of another Customer Account that is distinct from the account from which the agreement originated.

3.3 Terminology from Regulations

Digital Signature	An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the Signer and the integrity of the data can be verified. [21 CFR Part 11 Definitions]
Electronic Record	Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system, and subject to 21 CFR Part 11 requirements. [21 CFR Part 11 Definitions]
Electronic Signature	A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. [21 CFR Part 11 Definitions]
GxP	Generic acronym for compliance standards including but not limited to, Good Clinical Practice (GCP), Good Laboratory Practice (GLP), Good Manufacturing Practice (GMP), Good Distribution / Documentation Practice (GDP), and Good Pharmacovigilance Practice (GVP).
Predicate Rule	Any requirement set forth in the Federal Food, Drug and Cosmetic Act, the Public Health Service Act, or any FDA regulation other than 21 CFR Part 11.
Signature Appearance	A graphic that accompanies the signature manifestation and that identifies the Signer.
Signature Manifestation	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: The printed name of the signer; The date and time when the signature was executed; and The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

Note: While a "digital signature" is a form of "electronic signature", not all electronic signatures are digital signatures. Within this handbook, the term "electronic signature" will be used universally to designate all types of signatures applied using Acrobat Sign Solutions. The term "digital signature" will be used exclusively when referring to a signature process where identification verification and issuance of a digital certificate is performed by an external trust services provider. For additional information about digital signatures, you can go here.

4 Acrobat Sign Solutions in a GxP-Regulated environment

4.1 Getting Started

The implementation of Acrobat Sign Solutions for the application of 21 CFR Part 11 and/or EudraLex Annex 11 electronic signatures involves putting in place technical and procedural controls to meet regulatory requirements and business process needs. Acrobat Sign Solutions is designed to offer flexibility to its customers, empowering the customers to decide for themselves which features to use. It is important to understand the features available in Acrobat Sign Solutions to be able to make informed decisions related to the system configuration and necessary supporting processes.

Customers who have purchased Adobe Acrobat Sign Solutions, enterprise or business levels of service, can use the Adobe Admin Console to manage users, products, and Adobe entitlements across the entire organization. As soon as the contract has been purchased, the contract owner will receive an email from Adobe informing them that they have access to the Adobe Admin Console. Acrobat Sign Solutions plans can be purchased on a Per-User or a Per-Transaction basis, and this is reflected in how Acrobat Sign Solutions appears in the Admin Console.

While the user management and provisioning of access can be managed in the Adobe Admin Console, the Acrobat Sign-specific set up is done within the application itself. Before Acrobat Sign Solutions can be used, an Administrator must set up the account and configure it to meet the customer's business needs. The set-up and configuration is managed by an individual (or group of individuals) given the Admin role in Acrobat Sign Solutions.

Some legacy Customers may have onboarded in a manner that does not use the Adobe Admin Console. These Customers will administer their Acrobat Sign Solutions account and users entirely from within the application interface.

Learn more about getting started with Acrobat Sign Solutions here: https://www.adobe.com/go/sign-admin-guide

4.2 Use the *Bio-Pharma Settings* to Support 21 CFR Part 11 Requirements

Overview

In Acrobat Sign Solutions, the settings known as *Bio-Pharma Settings* include configuration parameters that are tied to meeting 21 CFR Part 11 requirements.

Learn more about how Acrobat Sign Solutions can meet the requirements of 21 CFR Part 11 and Annex 11 here: https://www.adobe.com/go/shared-responsibilities-cfr21-part11-annex11

The *Bio-Pharma Settings* alone are insufficient to satisfy all 21 CFR Part 11 requirements, but they are necessary to control different components of the signing ceremony that are critical to uniquely identifying a signer and that impact the signature manifestation. The *Bio-Pharma Settings* are used to:

- Enable identity challenges and specify when those challenges occur (e.g., upon opening the document, clicking on a signature field, completing a signature ceremony).
- Enforce the use of signing reasons and manage a pre-defined list of reasons to choose from.

When using *Bio-Pharma Settings*, the signature field is reformatted so that the printed name of the signer, the date and time of signature, and the specified reason for signature are systematically printed in the signature manifestation. The use of *Bio-Pharma Settings* is discussed in greater detail Using the Bio-Pharma Settings to Configure the Signature Manifestation.

Considerations

The *Bio-Pharma Settings* allow configuration of the signature ceremony to require multiple authentications of the signer to assure their identity throughout the signing process. You can think of this in terms of an individual showing identification when entering a building, and again when entering a specific office or secure area that they work in. With *Bio-Pharma Settings*, it is possible to require the signer to authenticate when they open the document, and again every time they initiate a signature within that document.

The *Bio-Pharma Settings* are available to customers who subscribe to Adobe Acrobat Sign Solutions, enterprise or business levels of service.

Learn more about configuring *Bio-Pharma Settings* here: https://www.adobe.com/go/adobesign-bio-pharma-overview

In addition to *Bio-Pharma Settings*, Healthcare and Life Science organizations that are concerned with protecting Protected Health Information (PHI) in compliance with HIPAA will also implement privacy and security safeguards within Acrobat Sign Solutions. There are options to enforce password policies, to automatically log users out of their web session after a period of inactivity, and to exclude email attachments. Customers are advised to consider these options and to review all their security settings before processing any protected health information (PHI) in Acrobat Sign Solutions.

Before processing protected health information through Acrobat Sign Solutions, the organization must enter into a Business Associate Agreement (BAA) with Adobe.

Learn more about HIPAA configurations and signing a Business Associate Agreement (BAA) with Adobe here: https://www.adobe.com/go/adobesign-hipaa-settings

4.3 Setting up the Account with Groups

Overview

In Acrobat Sign Solutions, the Account Administrator can create groups within the account. The group structure allows for the granular configuration of settings, creating a unique experience for the members of the group. This can be extremely useful for defining classes of users who need to send out agreements with specific signature requirements.

Learn more about adding and managing groups here: https://adobe.com/go/sign-groups-overview

Upon the creation of a new group, the group inherits the account-level settings. However, a group can be configured so that specific account settings are overridden at the group-level, making it possible to configure *Bio-Pharma Settings* at the group-level for certain group(s) only.

When business processes need to meet 21 CFR Part 11 requirements for electronic signatures, a dedicated group should be created and configured to use *Bio-Pharma Settings*. Authorized members of this group can send agreements to internal and external recipients for signature with *Bio-Pharma Settings* enforced. This setup is illustrated below.

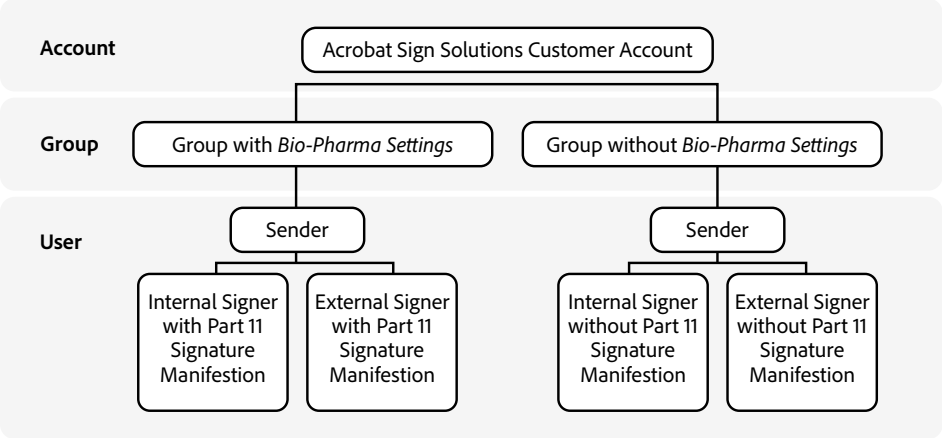

Figure 1 – Group Structure in the Acrobat Sign Solutions Customer Account

When an agreement originates from a group that has the settings for *Enforce identity authentication* enabled within the *Bio-Pharma Settings*, the recipients will be challenged to reauthenticate to Acrobat Sign Solutions at multiple instances during the signing process. Members of a group that uses *Bio-Pharma Settings* will also be required to reauthenticate whenever they are the only Signer on the agreement using the self-signing feature initiated from that group.

4.3 Setting up the Account with Groups

continued

Multiple reauthentication during the signing process impacts overall productivity and user experience. This is acceptable and unavoidable when trying to achieve 21 CFR Part 11 requirements for electronic signatures. However, not all business processes need to meet 21 CFR Part 11 requirements. In these cases, users should be added to a group that does not use the *Bio-Pharma Settings*. There is also an option to add users to multiple groups, so they can choose when to start transactions that yield 21 CFR Part 11 signature manifestations as well as other transactions.

Considerations

21 CFR Part 11 regulations only apply to electronic records and electronic signatures that are created, maintained and/or submitted to the FDA according to an FDA predicate rule (see definition in Glossary of Terms–Terminology from Regulations). Customers should perform an analysis of their business processes to establish what type of documents will need to be signed using Acrobat Sign Solutions with *Bio-Pharma Settings* and those that do not. While planning the implementation of business processes that use Acrobat Sign Solutions, segregate the business processes impacted by 21 CFR Part 11 from those that are not, and then create groups to separate users of different business processes from one another.

Even if only one business process is identified initially, it is advisable to architect the account with a group structure so that scalability will be possible in response to future organizational needs.

4.4 Adding Users to the Account and Groups

Overview

The Acrobat Sign Solutions account and user access can be managed through two distinct administrative environments:

(1) The Adobe Admin Console:

When a Customer is onboarded, the first administrator is given access to the Admin Console and from there, additional administrators can be assigned. The administrator can manage users, their identities, and licenses across all Adobe products and services. User creation can be managed manually or automated through synchronization with your organization's enterprise directory.

From the Admin Console, the administrator can grant/revoke a user's access to the Acrobat Sign Solutions product and assign one of three authority roles: User (with no administrative authority), Sign Account Admin, Sign Account and Privacy Admin. The assignment of Acrobat Sign Solutions group membership and user permissions must then be managed from within the administrative environment of the Acrobat Sign Solutions account.

(2) The Acrobat Sign Solutions application:

From within the application, a user who is assigned administrator privileges in Acrobat Sign Solutions can manage configuration settings, features, and functionality of the application.

Acrobat Sign Solutions administrators can also create and edit groups, assign users to group(s), and edit user permissions. Initially, when an end user or administrator is granted access to Acrobat Sign Solutions, that user is placed into the Default group in the account. However, an Acrobat Sign Solutions account administrator can move that user to another group within the account or assign them membership in multiple groups. Note that groups in Acrobat Sign are distinct from Adobe Admin Console user groups.

Legacy Customers who have onboarded without access to the Adobe Admin Console will administer their Acrobat Sign Solutions account and users entirely from within the application interface. These Customers can contact Adobe if they wish to have their account migrated to the Adobe Admin Console. In contrast, new customers will only be set up using the Adobe Admin Console which provides additional benefits.

Note that an Admin Console administrator is not necessarily an administrator of the Acrobat Sign Solutions account, as those administrative roles are independent of each other.

Once a user is created, a user profile is generated in Acrobat Sign Solutions to capture personal information. The user profile ties the individual's first and last name to a valid email address. The user will use this email address to identify themself to the Acrobat Sign Solutions service. Upon creation of the user account, the user will receive an email notification prompting them to log in to Acrobat Sign Solutions and may be required to accept the terms of use. The user will also be prompted to create a password at this time (unless the user is logging in with a federated ID).

Learn more about adding and managing users here: https://www.adobe.com/go/sign-add-users-to-account and https://helpx.adobe.com/enterprise/using/manage-users-individually.html#add-users

4.4 Adding Users to the Account and Groups *continued*

Through the user profile, an administrator may place the user in one or multiple groups. When the "Users in Multiple Groups" feature is enabled, users who are assigned Send privileges in multiple groups are allowed to send agreements from more than one group, with the Sender having the authority to decide which group an agreement originates from. This is especially important because the configuration settings associated to the Sender's group largely dictate the system-controlled properties (such as authentication methods, branding, PDF security) of the agreement. The Signer's experience will be dictated by the group-level settings of the group that the agreement originates from, irrespective of the group that the Signer belongs to. Failure to send an agreement from a group that is configured to generate compliant signatures will result in the collection of signatures that do not comply with the regulations.

Learn more about Users in Multiple Groups here: https://adobe.com/go/sign-umg-overview

Considerations

Acrobat Sign Solutions differentiates users by their unique email address. An email address can only be associated with a single Acrobat Sign Solutions account. Once a user is created in a Customer Account, that individual cannot be associated with a different Acrobat Sign Solutions account using the same email address. If an individual must be an active member of multiple Acrobat Sign accounts, they will require multiple unique email addresses. Errors during on-boarding users are usually the result of this requirement and can be resolved by contacting Adobe support to remove any conflicts that exist with the user's email address.

Administrators can leverage the user provisioning report in the Users page to help understand and resolve user creation issues. Any user who was not provisioned successfully will be listed as Pending, and recommended actions to resolve the issue will be suggested.

Customers should implement processes to ensure a unique email address is attributed to an individual prior to onboarding a user into the Customer Account.

Appropriate procedural controls should also be put in place to ensure individuals have met all organizational requirements and completed the necessary training prior to being assigned a user account in Acrobat Sign Solutions.

To provide non-repudiation and avoid the risk of fraudulent signatures, 21 CFR Part 11 requires that an individual's identity be verified before that individual is assigned an electronic signature. Organizations should implement a suitable identification verification process to confirm a person's identity (i.e., the person is who they claim to be) before onboarding a user into the Customer Account. This verification is usually performed just once by the customer or a trust service provider (TSP) and is carried out by validating an official ID document (e.g., passport, driver's license) or other piece of personally identifiable information. For practical reasons, many organizations couple the identification verification process with employee hiring and onboarding activities.

When a Sender belongs to multiple groups, one group must be marked as the user's primary group whose properties will be applied by default when the Sender accesses the Send page. The Sender is responsible for retaining the primary group or selecting a different group (and all settings associated with that group) that influence the Signer's experience and the properties of the resultant signatures. Following a conservative approach, it is advised to assign the group configured with *Bio-Pharma Settings* as the Sender's primary group. This approach is meant to avoid the unintentional collection of non-compliant signatures due to the Sender's failure to send the agreement from the appropriate group.

4.5 Apply and Manage User Permissions

Overview

Once a user is created in the Customer Account, the *Users* settings can be configured to assign them elevating levels of authority which grant the ability to sign documents (*Signer* role) and send documents for signature (*Sender* role at the group-level). Higher-level administrative functions can also be assigned, such as group, account and privacy administrator roles.

A user can only see agreements that they participate in (i.e., agreements sent by them and sent to them), but the Sharing feature can be used to expose agreements from other users to a given user (refer to Sharing Accounts and Agreements).

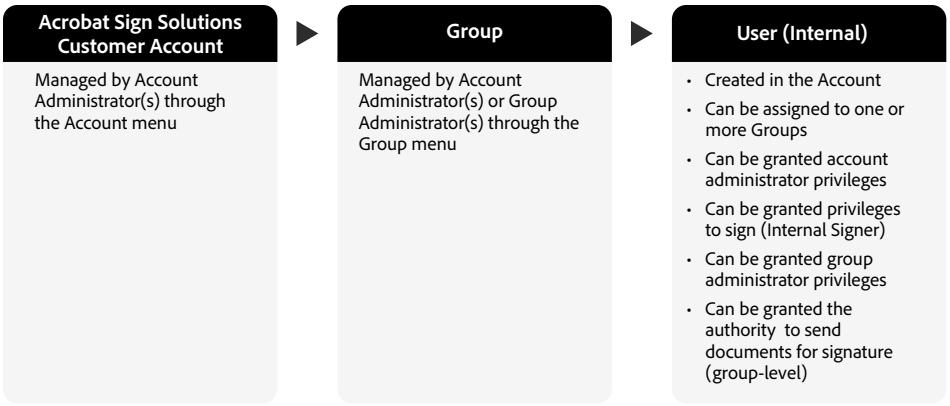

Figure 2 – Relationship between Account, Group, and User in Acrobat Sign Solutions

Learn more about editing a user's authority level here: https://www.adobe.com/go/adobesign-admin-roles

Sender

A Sender is a user who has the authority to send an agreement through the Acrobat Sign application interface to one or more recipients. The *Send* configuration settings associated with the Sender's group are applied and control the document signature process. When the Sender is a member of more than one group, the Sender can decide from which group an agreement originates.

4.5 Apply and Manage User Permissions

continued

Signer

Internal Signer

A user in the sender's Customer Account who has been assigned permission to apply electronic signatures is referred to as an *Internal Signer*. These users have limited system access. From their Manage page in the Acrobat Sign application interface, an Internal Signer can view and retrieve all the agreements that have been sent to them.

Typically, Customer Accounts are set up such that Internal Signers use their organization's Identity Provider (IdP) and Single Sign On (SSO) to identify themselves to the Acrobat Sign Solutions service during the signature process. While it is possible to set up a customer account to require Internal Signers to identify themselves to the Acrobat Sign Solutions service using other authentication methods, these methods are less practical and less commonly implemented.

External Signer

An individual does not need to be a member of the Customer Account with signing privileges to sign an agreement. *External Signers* can be signers with a user account in another Customer Account or can be signers with no Acrobat Sign user account at all. Any *External Signer* can sign an agreement sent to them through Acrobat Sign Solutions. External users gain access only to the agreements which they are requested to sign; they do not gain access to the Acrobat Sign application interface from where agreements are sent and managed. Given the identity authentication requirements of compliant signatures, External Signers can use an ID created with Adobe as their identity authority. For information on authentication methods available for External Signers, please refer to Identity Authentication Methods for Electronic Signatures.

Administrators (Account, Group, Privacy)

Account Administrator(s) have full authority to edit account settings and group settings for every group within their account. The Account Administrator has the authority to add/remove users (for legacy Customer Accounts only), create new groups, and appoint group administrators. Group administrators can be given the authority to add users to their group and change their group's settings to override those set at the account level. Account configuration settings control what actions a Group Administrator can perform.

Learn more about adding users in groups here: https://www.adobe.com/go/sign-add-users-to-groups

Multiple individuals can be assigned to Account Administrator and Group Administrator roles. However, the Group Administrator must be a member of the group for which they are acting as a Group Administrator. Some organizations may choose to forego the Group Administrator role. In the absence of a group administrator, the Account Administrator retains the authority to manage groups and group settings.

Additionally, an Account Administrator can be assigned the Privacy Administrator role to enable the removal of users and agreements from the account. The Privacy Administrator role can only be assigned to a user who is an Account Administrator.

4.5 Apply and Manage User Permissions

continued

Table 1: Administrator Responsibilities

Authority	Administrator (from Admin Console)	Account Administrator (within Acrobat Sign Solutions)	Group Administrator
Add new users to the account	X	[x]*	[x]*
Deactivate/reactivate users in the account	X	[x]*	
Remove users from the account (via Privacy Administrator role)		X	
Edit user profile		X	X
Create groups		X	
Add users to a group		X	X
Assign the Account Administrator role to a user	X	[x]*	
Assign the Privacy Administrator role to a user	X	[x]*	
Assign the Group Administrator role to a user		X	X
Assign the Sender role to a user		X	X
Assign the Signer role to a user (Internal Signer)		X	X
Manage account settings		X	
Manage group settings		X	X

* For legacy Customers who have onboarded without access to the Adobe Admin Console, the addition/removal of users and assignment of administrator privileges can be accomplished within the Acrobat Sign Solutions application interface.

4.5 Apply and Manage User Permissions

continued

Considerations

For GxP business processes, appropriate procedural controls should be put in place to ensure that the Sender only requests signatures from Signers who have met all the organizational requirements authorizing them to sign controlled documents using electronic signatures. These procedural controls may include user training and/or maintaining a user access list that Senders can consult to determine which individuals are permitted to apply electronic signatures.

If your organization is using Acrobat Sign Solutions to send agreements as part of both GxP and non-GxP business processes, the use of the group structure is recommended so that *Bio-Pharma Settings* can be applied to specific groups whose members must participate in those business processes to which 21 CFR Part 11 applies. The configuration settings associated to the Sender's group are applied during the signature process. Therefore, it is important to ensure that individuals who will act as Senders are assigned to a group that is configured to use *Bio-Pharma Settings*.

When using Acrobat Sign Solutions for GxP business processes, your organization should also assess whether:

- Appropriate supporting processes are in place to govern the controlled operation of the system and how configuration of the Acrobat Sign Solutions account is managed, ensuring that the *Bio-Pharma Settings* are maintained and applied when signing controlled documents with GxP regulated content.
- Controls are implemented to make sure that users in groups configured to use *Bio-Pharma Settings* meet all your organization's requirements for participating in GxP business processes. For example, you may decide to restrict group membership to users with corporate credentials, who in turn have completed internal onboarding and identification verification processes.

4.6 Signature Types

Overview

Acrobat Sign Solutions supports *electronic signatures* that meet the requirements of the *ESIGN* Act as well as the *eIDAS Regulation* and many other e-signature regulations worldwide. Acrobat Sign Solutions also supports the more secure, Qualified Electronic Signature (QES) or *digital signatures* using a certificate-based digital identifier to confirm the signer's identity. Organizations can implement the signature type method that best fits their risk profile or that best supports their use cases.

Learn more about global e-signature laws here: https://adobe.com/go/trust-compliance-cloud-signatures

When implementing certificate-based digital signatures, an external trust services provider (TSP) will need to be selected. The trust service provider is an entity that is responsible for the creation, verification, and validation of digital signatures. Acrobat Sign Solutions supports the trust service providers identified in the Adobe Approved Trust List (AATL) and the European Union Trust List (EUTL).

Learn more about approved trust service providers here: https://www.adobe.com/go/digital-id-providers and https://helpx.adobe.com/document-cloud/kb/european-union-trust-lists.html

The Acrobat Sign account can be configured to accept cloud signatures, i.e. digital signatures where the signer's digital certificate is managed by a trust service provider (TSP) and is securely stored in the cloud. Acrobat Sign Solutions supports the trust service providers that are members of the Cloud Signature Consortium (https://cloudsignatureconsortium.org/), an organization that defines a universal open standard for cloud-based digital signatures.

Learn more about cloud signatures here: https://www.adobe.com/go/adobesign-config-cloud-signature-providers

Considerations

If choosing to use the cloud-based digital signature functionality, an external trust services provider will need to be selected and paid for separately. The Customer's vendor management procedures may require a formal assessment and proper due diligence of the trust service provider in order to ensure that they comply with the Customer's quality and service expectations.

Learn more about Acrobat Sign Solutions digital signatures here: https://helpx.adobe.com/sign/config/digital-signatures/overview.html

Obtaining a physical (wet ink) signature is sometimes unavoidable. Acrobat Sign Solutions can be configured to support obtaining written signatures while ensuring proper access control and leveraging the convenience and benefits of electronic processing and auditing.

Learn more about obtaining written signatures here: https://adobe.com/go/obtain-written-physical-signature

4.7 Identity Authentication Methods for Electronic Signatures

Overview

Identification is the act of presenting some record or qualifying personal information to confirm a person's existence. In comparison, identity authentication involves verifying the person's identity and some additional information to determine if the person is who they say they are. The simplest method is Single-factor authentication, and this is commonly achieved by checking one's identity claim (e.g., username) against only one "factor" (e.g. password). With multi-factor authentication, the robustness of the authentication is augmented with the enforcement of more "factors", which generally rely on at least one of the following: something you have – such as a token or device, something you know – such as a password or PIN, something you are – such as fingerprint or other biometrics.

Learn more about identity authentication methods in Acrobat Sign Solutions here: https://www.adobe.com/go/adobesign-authentication-methods

Acrobat Sign Solutions is designed to offer flexible authentication methods that meet the needs of diverse business processes. Identity authentication methods supported in Acrobat Sign Solutions are described in the table below. Organizations can select and implement the authentication method(s) that best fit their risk profile or that best support their use cases and budgetary allowances. "Premium" authentication methods require additional license terms and subscription fees to use with the application.

4.7 Identity Authentication Methods for Electronic Signatures *continued*

Table 2: Identity authentication methods

Method	Description	Availability	Premium ($)	Enforced authentication via BioPharma Settings is supported
Single-factor				
Acrobat Sign authentication	Prompts the recipient to validate their identity by logging in with a valid ID created with Adobe (email address and password)	Business and enterprise only	No cost	Yes
One-Time Password via Email (OTPvE)	Prompts the recipient to enter a single-use passcode that is retrieved from the recipient's email inbox	Business and enterprise only	No cost	Yes
Two-factor				
Password based authentication	Prompts the recipient to enter a signing password that is defined by the sender when setting up the agreement	All service plans	No cost	No
Knowledge-based authentication (KBA)	Prompts the recipient to correctly answer personal questions, e.g. "What is your mother's maiden name?"	Business and enterprise only, Only for recipients in USA	Incurs additional per-use fees	No
Phone authentication	Prompts the recipient to enter a verification code that is sent to their phone via SMS or voice call	Business and enterprise only	Incurs additional per-use fees	Yes
Government ID	Instructs the recipient to supply a selfie image and an image of a government-issued document (driver's license, passport)	Enterprise only	Incurs additional per-use fees	No
Cloud-based Digital Signatures	Requires a signer to authenticate to a third-party identity provider who verifies signer identity and issues the certificate-based digital IDs used to apply a digital signature	All service plans	Incurs additional per-use fees	Yes

4.7 Identity Authentication Methods for Electronic Signatures *continued*

If no *(None)* authentication is selected, Acrobat Sign Solutions relies solely on email to verify the recipient, considering that email addresses are unique and password-authenticated. If an agreement is sent with no *(None)* authentication (previously listed as *Email* authentication in earlier versions of Acrobat Sign Solutions), clicking the hyperlink in the email will open the agreement directly for viewing and action by the recipient (without further authentication). To finalize the signature, the recipient simply clicks on the *Click to Sign* button without any further authentication. Customers should apply proper governance procedures to ensure access to email inboxes is controlled according to best practices for information security.

Proper authentication methods are necessary to meet 21 CFR Part 11 requirements pertaining to authorization. While no *(None)* authentication is sufficient for many business needs, the *Acrobat Sign* authentication method is preferred for business processes that require an authenticated event for each signature. With *Acrobat Sign* authentication, recipients are asked to authenticate to Acrobat Sign before they can view the agreement contents (unless they are already logged into Acrobat Sign Solutions).

Given the challenges of identifying individuals with electronic signatures, Customers may choose to use cloud-based digital signatures in a regulated environment. If certificate-based digital signatures are not chosen for use in the business process, it is judicious to use multi-factor authentication. Acrobat Sign Solutions supports two-factor authentication methods to verify the identity of a Signer. If an agreement is sent with two-factor authentication, clicking the hyperlink in the email will prompt the user to validate their identity prior to opening the agreement for viewing and action.

For business processes where 21 CFR Part 11 applies, *Bio-Pharma Settings* are used to require Signers to provide valid credentials several times during the signature process. Based on configuration options for *Enforced Identity Verification*, the Signer may first be challenged prior to opening the agreement, next when the signature field is clicked, and finally when the *Click to Sign* button is pressed. Each identity challenge can be controlled separately and enforced as a unique challenge.

Any of the implemented methods (as selected in the *Send settings*) can be selected when setting up the agreement. However, the Sender must be aware that the enforced authentication controlled by *Bio-Pharma Settings* requires one of the following compatible authentication methods:

- **Phone authentication:** Phone authentication ties the Signer to a known physical phone device supplying the necessary second level of identity authentication. This method requires signers to enter a verification code that is sent to their phone (via SMS or voice call) before being allowed to view the agreement content and sign a document. There is a cost consideration for the use of Phone authentication. An additional charge is applied when this method is used. These fees are negotiated as part of your Acrobat Sign Solutions license agreement and are accounted for as part of the subscription fee for the service. Phone authentication transactions must be purchased before use and are consumed on a per-recipient basis.

4.7 Identity Authentication Methods for Electronic Signatures *continued*

- **Acrobat Sign authentication:** Acrobat Sign authentication either uses the identity provider of the account (when SSO is enabled) or uses an ID created with Adobe for authentication. With this method, Signers are required to provide valid credentials, consisting of their verified email address or an Adobe ID and password before being allowed to view the agreement content and sign a document. There are no additional fees for using the Acrobat Sign authentication method.

- **One Time Password via Email (OTPvE) authentication:** This method requires signers to enter a verification code that is sent to their email inbox before being allowed to view the agreement content and sign a document. As the email address is known to the system, this information is prefilled. There are no additional fees for using the OTPvE authentication method.

Learn more about enforced identity verification here: https://adobe.com/go/enforce-identity-authentication

While the *Bio-Pharma Settings* explicitly define where in the agreement the Signer will be challenged to authenticate themselves, the experience is dictated by the identity authentication method(s) specified within the Send Settings for the account or group. The Send Settings allow Customers to configure preferences for identity authentication as well as other parameters on the Send page interface. As part of the Send Settings, the administrator can control the authentication methods available to the Sender and determine if the Sender should be allowed to change from the default method. These settings are applied at the account level but can be overridden at the group level.

Default identity authentication methods can be defined for Internal and External Signers. It is possible to define different default methods for these two categories of Signers. For example, External Signers might always be required to use Phone authentication or to use an Adobe ID while Internal Signers might always default to using Acrobat Sign authentication with SSO enabled to authenticate.

If using the cloud-based digital signature functionality, the chosen identity authentication method will be enforced and additional credentials issued from a trust service provider (e.g., personal identification number (PIN) or one-time password (OTP)) will be requested from the Signer at the time of signing.

Acrobat Sign Solutions' Digital Identity Gateway provides additional authentication options available for a fee. The Digital Identity Gateway allows organizations to deploy pre-configured third-party digital identity providers (IdP) and leverage their authentication and signer identity verification services using the standard OpenID Connect (OIDC) authentication protocol. However, the Digital Identity Gateway presently does not support enforced authentication controls enforced via *Bio-Pharma settings* and should be excluded from 21 CFR Part 11 implementations of Acrobat Sign Solutions.

Learn more about Acrobat Sign Solutions' Digital Identity Gateway here: https://www.adobe.com/go/sign-config-digital-identity

Considerations

Cost is a consideration when choosing the appropriate identity authentication method. Using the *Acrobat Sign authentication* method can provide both a secure and no-cost method when *Phone* authentication is impractical. *Acrobat Sign authentication* can be used for both Internal and External Signers.

An Internal recipient is (by definition) a member of the Customer Account and, therefore, is "known". In this scenario, using the *Acrobat Sign authentication* method is a "frictionless" option without the additional costs associated with premium authentication transactions.

4.7 Identity Authentication Methods for Electronic Signatures *continued*

Using the *Acrobat Sign authentication* method with External recipients presents a unique challenge because they may or may not have an ID with Adobe. If they do not, they will be required to register. This may introduce a level of "friction" and can cause frustration for the recipient. In the scenario where the External Signer is "unknown", using the *OTPvE* method (single-factor) or the *Phone* authentication method (two-factor) may be preferred.

Scenario 1: The Recipient is an Internal Signer

An organization's SSO capabilities are best suited to verify the identity of the Internal Signer. Positive identity and straight-forward authentication can be accomplished using the Customer's own Identity Provider (IdP) that is configured to work with Acrobat Sign Solutions. SSO is an ideal choice for enterprise customers and organizations who need greater control over how users access software applications. Refer to Using Single Sign-On (SSO) for User Authentication for further information.

Some organizations have policies or technical constraints that discourage the implementation of SSO. In these circumstances, the Customer Account can be configured to use the *Acrobat Sign authentication* method, prompting the recipients to authenticate using a verified email address and password (ID with Adobe).

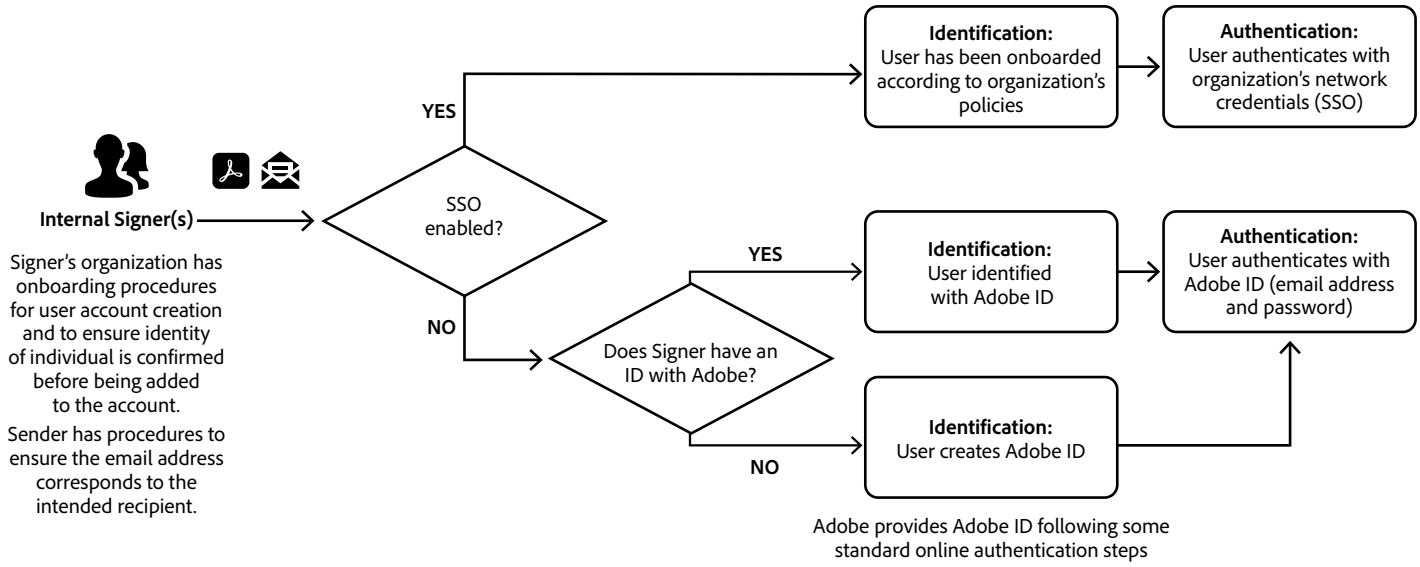

Figure 3 – Authentication Process for Internal Signers

4.7 Identity Authentication Methods for Electronic Signatures *continued*

Scenario 2: The Recipient is an External Signer

For External Signers, the use of *Phone authentication* is ideal if their phone number is known and confirmed to belong to the Signer. The Sender must know the phone number at send time; the recipient's phone number must be entered by the Sender when setting up the agreement. To electronically sign a document, the External Signer must access the agreement via a link from their email inbox. To view the contents of the agreement, the recipient must provide a system generated verification code sent to their phone number. The Signer can choose to receive the verification code by SMS (text message) or via voice call. Since a new verification code is generated by the system every time the user needs to be authenticated, the use of the *Phone* authentication method ensures that no two signing activities use the same combination of credentials.

When the recipient is an External Signer and their phone number is unknown or cost is a factor, the *Acrobat Sign authentication* method can be leveraged. Adobe can provide a new personal ID with Adobe (called Adobe ID) to support authentication during signing. In the case where the Signer lacks an ID with Adobe, the individual will be prompted to create one before being allowed to view the agreement. This involves registering and validating the individual's email address and can also include associating a phone number to the account (to facilitate password recovery). The ID is free and can be used to access other Adobe products and services if desired. However, there is no obligation to participate further with Adobe beyond the signing ceremony. While this is not the recommended approach, some Customers have implemented this method in conjunction with suitable processes to ensure the identification of the individual is verified. Refer to Implications for External Signers for further information.

The *OTPvE* method is another no-cost option that can be leveraged for External Signers. With this method, the users are not required to create an ID with Adobe. They simply need access to their email inbox, eliminating much of the friction that could arise with the *Acrobat Sign authentication* method.

An individual is considered an External Signer because they are not a licensed user within the Customer Account that the agreement originated from. However, it is possible that this individual is a member of an Acrobat Sign Solutions account belonging to a different customer entity. If the account that the Signer belongs to is configured with SSO, then the Signer can use their organization's network credentials to authenticate.

4.7 Identity Authentication Methods for Electronic Signatures *continued*

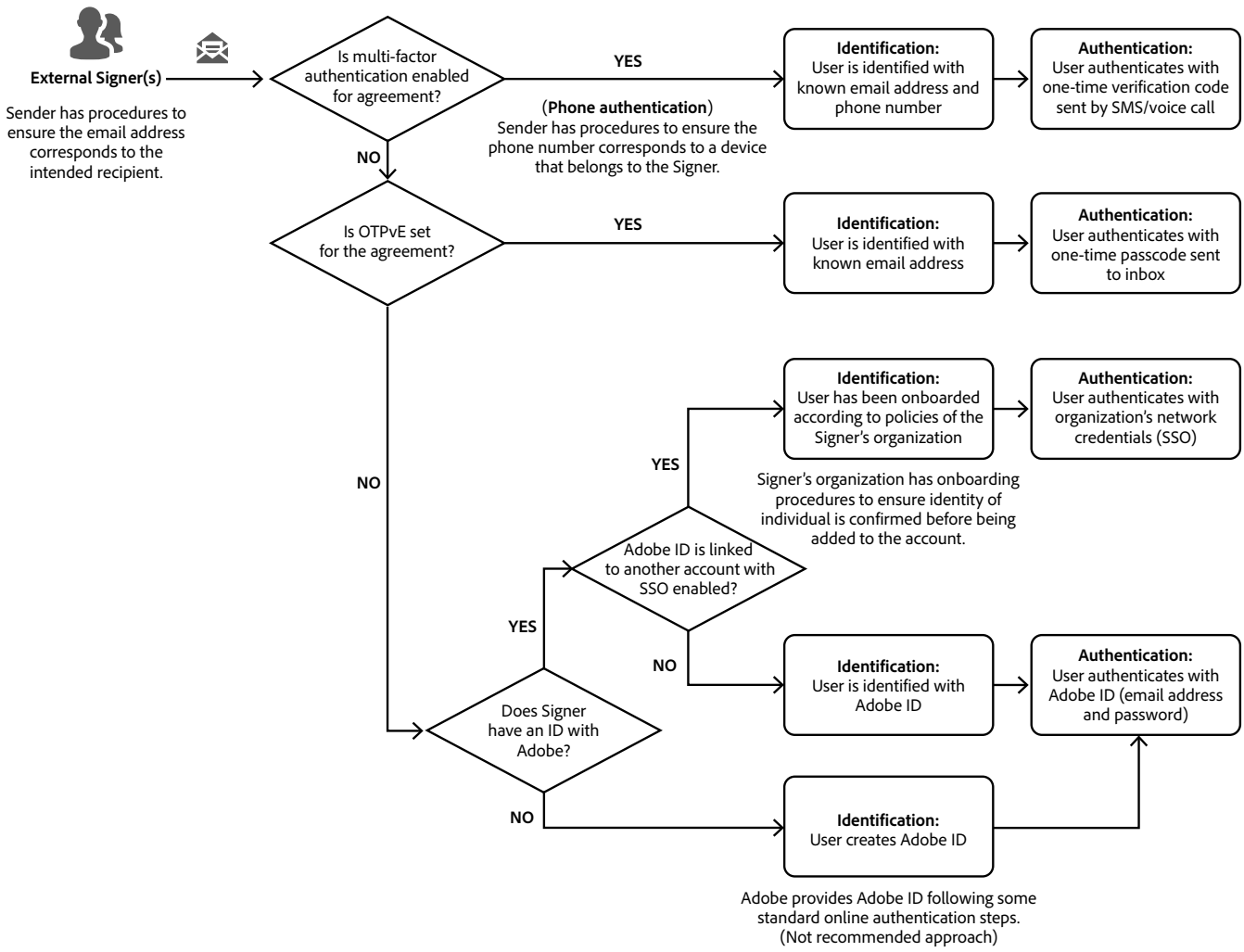

Figure 4 – Authentication Process for External Signers

4.8 Using Single Sign-On (SSO) for User Authentication

Overview

When managing an Acrobat Sign Solutions account on the Admin Console, an administrator can set up the account and configure domains which are used for login via the Federated ID identity type for SSO. Once the domain is verified, the directory containing the domain is configured to allow users to login to Acrobat Sign Solutions using an email address within that domain via an Identity Provider (IdP), such as Microsoft Entra ID, Google Federation, or Okta.

Learn more about setting up identity in the Adobe Admin Console here: https://helpx.adobe.com/enterprise/using/set-up-identity.html

Automatic user account creation for an existing directory can be facilitated by enabling just in time (JIT) provisioning. Once enabled, Customers will be able to set up automatic assignment rule(s) that assign Adobe Acrobat Sign product entitlement to a federated user without further action from an administrator.

Learn more about just in time (JIT) provisioning here: https://helpx.adobe.com/sign/admin/jit-via-sso.html

If not using the Adobe Admin Console, an administrator can configure *SAML Settings* within the Acrobat Sign Solutions application. This allows for SSO to be enabled for the authentication of users in your account. *SAML Settings* are applied at the account level only and cannot be overridden at the group level. An Enterprise plan is needed to apply *SAML Settings*.

Considerations

Federated IDs are recommended for customers who want to maintain strict control over authentication and users based on identity management system(s) that are already in place within the organization. The organization's directory services can be used to manage password and user account lockout policies for Internal users. Logs can be monitored by the Customer to detect and report unusual or suspicious activity on user accounts. Moreover, from the end-user's perspective, the log-in process is faster and easier since the end-user will be redirected to their organization's standard SSO experience which they are already familiar with.

If SSO is not used, users will be authenticated with user account credentials created within the Acrobat Sign Solutions service. In this mode, each user will receive an email notification upon creation of the user account, prompting them to log in to Acrobat Sign Solutions and accept the license entitlement.

Business level service plans do not support SSO. An enterprise plan is required.

Learn more about using the Adobe Admin Console to set up Single Sign-On (SSO) with your Identity Provider (IdP) here: https://helpx.adobe.com/enterprise/using/sso-overview.html

4.9 Implications for External Signers

Overview

Acrobat Sign Solutions determines if the recipient of the agreement is in your organization based on account membership. An External Signer is any recipient who is not a user in the Acrobat Sign Solutions account that the agreement originated from.

Sending a document to an External Signer is no different than sending an agreement to an Internal Signer. The Sender accesses the *Send* interface within Acrobat Sign Solutions and adds the list of intended Signer(s) by providing the recipient's (Internal and/or External Signers) identifying email address.

As the Sender must also specify the desired authentication method, the Sender needs to be aware that External Signers may require a different authentication method than Internal Signers. Default identity authentication methods defined within the *Send Settings* for Internal and External Signers can be used to ease this burden. For information on authentication methods available for External Signers, refer to Identity Authentication Methods for Electronic Signatures.

Considerations

Little configuration is necessary to allow External Signers to participate in the signature process. However, given that External Signers are not part of the Customer's account, multi-factor authentication methods should be used when possible for them to participate in regulated signature processes. The choice of authentication method depends on various factors, including cost, risk, and the compliance requirements of the process.

In some cases, with thousands of External Signers participating in the process (e.g., a public clinical trial), *Acrobat Sign authentication* using an ID created with Adobe is a viable option. For a smoother user experience, the OTPvE method is preferred. This provides a no-cost way to assure identity when only the email of the recipient is known to the Sender. In other cases, with a smaller number of well-known recipients and a higher business value, *Phone authentication* may be appropriate.

Customers should implement procedures to ascertain that the individual is the genuine owner of the email address and phone number (if applicable) used to receive and execute the signature request. Irrespective of the authentication method, Customers should implement processes to ensure the identification of the individual is verified (i.e. the person is who they claim to be) by validating an official ID document or other piece of personally identifiable information. Customers should be especially mindful of this before choosing to use the *Acrobat Sign authentication* method with External recipients. If the recipient does not already have an ID with Adobe, they will be required to register. Anyone with an email address can create an Adobe ID by following some standard online authentication steps, but there is no identification verification process to confirm a person's identity.

For GxP business processes, appropriate procedural controls should be put in place to ensure that the Sender only requests signatures from Signers who have proven their identity and satisfied other organizational requirements. These procedural controls may include training for Senders and/or maintaining a user access list that Senders can consult to determine which individuals have been vetted and are permitted to apply electronic signatures.

Individuals that act on behalf of the account or organization (such as contractors or vendors) can be onboarded into the Customer Account and participate as Internal Signers instead of being handled as External Signers. These individuals should be trained on organizational security policies and quality system procedures to meet all the business and regulatory requirements that permit them to sign documents as part of a GxP process. This approach may be especially practical if the individual will be expected to use Acrobat Sign Solutions on more than a single instance.

4.10 Setting up an Agreement

Overview

Only authorized users with permission to send documents for signature are given access to the *Send* page within the Acrobat Sign application interface. This is where Senders identify the intended recipients and select the files to be routed for signature. The interface is intuitive and the process for requesting signatures is the same for Internal and External Signers.

When the Customer Account has the User in Multiple Groups feature enabled, the group selector will be available. The Sender has the authority and the responsibility to choose which group an agreement originates from. To obtain signatures that comply with 21 CFR Part 11 requirements, the Sender must choose to send the agreement from a group that is configured with *Bio-Pharma Settings*.

Learn more about sending agreements here:
https://helpx.adobe.com/sign/using/sending/overview.html

Acrobat Sign Solutions can be configured to allow or restrict from where Senders can select the files to attach to the agreement. Files can be attached from the Sender's local system, cloud-based storage (Google docs, Box, Dropbox, OneDrive), or from the Acrobat Sign library. Several document and image file formats are supported.

The standard *Send* page can be used to identify one or more recipients, recipient groups, or simply to include oneself as the sole signer. In the *Send* page interface, the Sender provides each recipient's email address.

Based on configuration options for *Allowed Recipient Roles,* various recipient roles are available and can be assigned to accommodate the different ways in which the recipient can interact with the agreement. The "Signer" role will be pre-selected by default for each recipient, requiring them to apply at least one signature to the agreement. If the agreement needs to be signed in the presence of a witness, the "Sign with Witness" role can be assigned to the recipient, and this will prompt the Signer to identify the witnessing party who will be required to sign the agreement once the Signer completes their signature process.

The Sender can set up the agreement so that the recipients receive the signature request sequentially (in the order listed), in parallel (in no specific order), or in a hybrid order.

While preparing to send a document for signature, the Sender should enter the authoring environment, allowing them to preview the document and insert the required signature fields as placeholders for the expected signatures. Various electronic signature field types can be placed on a document, but the appropriate type should be selected to ensure the signature manifestation displays all the required elements per 21 CFR Part 11.

When using electronic signatures, the Sender should insert electronic signature fields of type *E-Signature* or of type *E-Signature Block (with email).* Each Signer can be assigned one or more electronic signature fields in a document. When *Bio-Pharma Settings* are configured, the *E-Signature Block (with email)* is adapted to ensure all the required information is displayed (i.e., printed name of the Signer, date and time stamp, reason for signing) as well as the Signer's email address.

When using certificate-based digital signatures, the Sender must enter the authoring environment and insert signature fields of type *Digital Signature* in the document. Cloud-based signatures can support up to 10 digital signature fields per recipient.

If the Sender does not position the signature fields through the authoring environment, Acrobat Sign Solutions will automatically set *E-Signature Block (with email)* fields for the Signers in positions assigned by the system.

Learn more about field types here:
https://helpx.adobe.com/sign/using/field-types.html

4.10 Setting up an Agreement *continued*

Considerations

A Sender who is also assigned signer privileges can use the *Send* page to upload a document that requires their signature alone. This method can be used as a valid alternative for the structured self-signing workflow which allows the Sender to sign a document alone without any other recipients.

The standard *Send* page is used by Senders who need to create and send ad hoc agreements, but other mechanisms exist to optimize the creation of agreements that fit specific business process requirements. The *Send in Bulk* feature can be used to send the same agreement to multiple recipients. The *Custom Send Workflow* designer allows for the standardization of agreement elements (such as recipient roles, signing order, files to be included in the agreement, etc.) so that the process of setting up an agreement is simplified for Senders. Additionally, advanced workflows can also be automated using seamless integration with Microsoft Power Automate.

Acrobat Sign Solutions has default limitations to accommodate normal usage volume and to ensure adequate performance thresholds. Senders should ensure that uploaded files do not exceed the allowable file size limit and the total page count threshold enforced by Adobe. Senders should be aware of the quota on the number of recipients that can be added to a transaction.

Learn more about transaction limits here:
https://helpx.adobe.com/sign/using/transaction-limits.html

If an agreement was sent out for signature and you realize that you need to make some modifications to the agreement after it was sent, there are several options available that allow the agreement to be modified or for the list of recipients to be adjusted:

- Acrobat Sign Solutions can be configured to allow the Sender to replace a recipient. This option allows the Sender to update any recipient who has not yet completed their action for the agreement (sign, approve, delegate, cancel or otherwise) by replacing the recipient's email address with that of a different recipient.
- There is no option to simply remove one recipient. However, Acrobat Sign Solutions can be configured to allow the Sender to add an alternate recipient. With this, the new recipient can take action on the agreement while leaving the original recipient in place and capable of participating in the agreement. The replacement of a recipient is reflected in the audit report.
- Acrobat Sign Solutions can be configured to allow the Sender to modify an agreement. This will allow them to make several types of changes, including adding/deleting/reordering documents and form fields. Keep in mind that there are some constraints. The ability to modify an agreement in flight is not possible if the agreement includes digital signatures and is not possible if a recipient has already performed their action for the agreement.
- The Sender can cancel the agreement at any time prior to completion. When canceled, the agreement will be voided and this will be captured in the audit report. Once voided, the Sender cannot restart the agreement; a new agreement would need to be initiated. Once all recipients have executed their signatures, the agreement is completed and can no longer be canceled.

4.10 Setting up an Agreement *continued*

- Acrobat Sign Solutions can be configured to offer recipients the option to decline to sign. When declined, the agreement will be voided and this will be captured in the audit report. Once voided, the Sender cannot restart the agreement; a new agreement would need to be initiated.
- An option can be configured to allow the current recipient to restart an agreement. When restarted, the agreement is returned to the first recipient and all signatures and initials applied to the document are removed. Then, the document will follow the normal signature process where each recipient will be notified in turn to take the required action on the document. Each recipient will be able to edit and correct any previously entered field data and complete their signature and initials once more.

When an agreement is sent, the recipients will receive an email informing them that the document is awaiting signature. By default, the email contains a hyperlink to the document. However, for organizations with stricter security policies that do not allow clickable links in emails, there is an option to send agreement emails without active links. Recipients will instead receive instructions on how to use an access code to gain access to the document in the signing environment.

Additionally, an option allows Senders to request signatures by delivering an agreement's URL directly to the recipient's smartphone via SMS (in addition to the standard email format). This is particularly useful when the recipient does not have easy access to their email inbox. When using SMS alone (as a replacement to the standard email format), the phone number is the sole identifier linked to the recipient. However, the phone number captured within the audit report is obfuscated (only the last four digits are exposed), which prevents unique traceability to the individual within the audit report entries. This can be resolved by using the option to display the full phone numbers in the audit report.

4.11 Using the *Bio-Pharma Settings* to Configure the Signature Manifestation

Overview

When using *Bio-Pharma Settings*, the system implicitly changes the layout of the signature manifestation. *Bio-Pharma Settings* can be configured to ensure that each signature manifestation includes the following components which are required by 21 CFR Part 11:

- The printed name of the signer
- The date and time when the signature was applied
- The signature meaning (reason for signing)

This information is displayed in human readable form on the electronic display and any paper printout of the signed document.

Learn more about configuring *Bio-Pharma Settings* here: https://helpx.adobe.com/sign/using/bio-pharma-settings-configuration.html

The printed name of the signer

For Internal Signers, the printed name of the Signer in the signature manifestation corresponds to the first and last name recorded in the user's Acrobat Sign User Profile (if using the *Acrobat Sign authentication* method). The system can be configured to prevent editing of the name by the Signer.

For External Signers, the signer will be prompted to type in their full name at the time of signing (unless the user is registered with Adobe). The typed name will appear in the signature manifestation. An option is available to allow the Sender to prefill the recipient's name when setting up the agreement and to prevent the recipient from modifying that name.

Learn more about the recipient's name here: https://helpx.adobe.com/sign/config/send-settings/require-recipient-name.html

If using certificate-based digital signatures, the printed name of the Signer matches the Signer's digital ID.

The date and time when the signature was applied

The time stamp in the signature manifestation is applied when the Signer presses the *Click to Sign* button. This action represents a positive acknowledgement from the Signer that he is willfully signing the document. At this moment, the file is "locked" and an entry is recorded in the agreement's activity log (audit trail) to capture the signing action. If the Signer is applying multiple signatures within a single agreement, he will press the *Click to Sign* button only once at the end of the agreement when the final signature is placed. Although the individual's signature will appear in multiple locations within the document, it is important to note that these signature manifestations essentially represent one signing event. The timestamp across the signature fields will be updated to the time when the *Click to Sign* button was pressed and only one entry will be captured in the agreement's activity log (audit trail) to reflect the moment at which the *Click to Sign* button was actioned. There may be other scenarios where operational requirements dictate the need to follow a sequential or chronological order of signing activities, in which case signing the document multiple times at once may not be suitable. In those cases, it may be more appropriate to enforce the sequencing of signing events by leveraging Acrobat Sign's built-in workflow capabilities and control the desired signing sequence specified by the Sender when setting up the agreement.

Date and time stamps in the signature manifestation are recorded in standard format, unless configured to use a specific format. For information on managing date format and time zone settings, refer to Date and Time Zone Settings.

4.11 Using the *Bio-Pharma Settings* to Configure the Signature Manifestation

continued

The signature meaning (reason for signing)

Bio-Pharma Settings can be configured to require the Signer to provide the reason for their signature. Moreover, it is possible to configure a picklist of reasons that the signer will be allowed to choose from and whether the signer will have the option to enter their own reason or be restricted to the list. At the time of signing, the Signer will be prompted to provide a reason for signing and will not be able to complete the signature unless a reason is entered. Once a reason is provided, the *Click to Sign* button will be exposed. The Signer must re-authenticate after pressing the *Click to Sign* button to allow for the electronic signature to be applied.

Learn more about enforcing a reason for signature here: https://helpx.adobe.com/sign/using/reason-for-signature.html

Considerations

Configure *Bio-Pharma Settings* at the group level. Reasons for signing in the *Bio-Pharma Settings* can be specified at the account level and will be propagated to all groups unless intentionally overridden at the group level. Consequently, any reasons for signing configured at account level may apply to all groups and additional reasons for signature set at group level will be added to the list of reasons.

When configuring the list of signing reasons, it is possible to categorize each reason by language. During the signing ceremony, only those reasons that match the Language value for the signer's locale will be presented for selection by the signer. It is also possible for the Sender to decide the signing language when setting up the agreement, and this will result in a list of reasons that is filtered on language for the recipient. If deploying in different geographical regions with unique language requirements, this feature may be leveraged to make reasons available in multiple languages.

The length of the signing reason text is limited. As the font size in the signature manifestation is scaled to fit into the signature field, it is recommended to keep the signing reason text as short as possible to ensure that the font size remains legible within the signature manifestation.

Implement controls to ensure the correct name is incorporated into the signature manifestation:

- For Internal Signers, procedures and controls for the management of the user profile information should be put in place. Consider utilizing a tool to synchronize the user's name with information in the identity management system used for SSO authentication. It is also possible to configure *Signature Preferences* that prevent recipients from changing their name in the signature panel during the signing ceremony.
- For External Signers, procedures should be put in place to ensure the individual understands the importance of providing a complete and accurate name at the time of signing.

All Signers must understand their responsibility in signing any agreements and must recognize that a reason for signing is necessary for a 21 CFR Part 11-compliant signature.

4.12 Signature Delegation

Overview

The configuration pertaining to delegation can be applied in the *Group Settings* and it is possible to prohibit delegation entirely for a specific group. *Delegation* can be controlled such that it may be permitted for Internal Signers only, External Signers only, or both.

When Internal Signers are permitted to delegate, additional configuration may be applied to control who their signature may be delegated to:

- Delegation to users in the Customer Account only (Internal Signers)
- Delegation to anyone whether inside or outside the Customer Account

When External Signers are permitted to delegate, their signature may be delegated to anyone.

The signature request can be delegated by the recipient or an auto-delegation can be assigned. When a signature is delegated to a new Signer, the Sender is informed via email. Auto-delegation can be set either by the user, an Account Administrator, or Group Administrator. All signature requests are automatically sent to the delegated Signer until the auto-delegation is removed.

Considerations

When delegation is permitted, procedural controls must provide instructions on when a signature can be delegated in a business process and to whom. The process controls should mitigate the risk of a signature request being delegated to an individual who is not authorized to sign controlled documents using electronic signatures.

4.13 Audit Trail Capabilities

Overview

For each agreement, Acrobat Sign Solutions provides a system-generated activity log (audit trail) that can be viewed and downloaded as an *audit report* in PDF format. The audit report includes entries for the sequence of events pertaining to the electronic signature collection process. The audit report also captures when a written signature was submitted, when a signature was delegated, when an agreement was canceled, when a recipient restarted an agreement, and when a Signer declined the request to sign. Audit report entries associated to the successful application of an electronic signature include the following information:

- Signer's name and email address
- Signature date and time
- Reason for signing

If declining to sign or canceling an agreement, the reason for declining or canceling is also captured in the audit report.

Additionally, each authentication event is captured in the audit report and will explicitly reflect the type of authentication used.

The audit report can capture the IP address of the device used to view the document being signed as well as the IP address of the time server used to record the signature timestamp.

If desired, the Customer Account can be configured to augment the audit report with additional details:

- Senders have the option to send periodic and ad hoc email reminders to recipients of an agreement. Reminder events can be included in the audit report to log when a reminder email is sent to recipients.
- Agreement view events can be included in the audit report. This will keep track of each time a participant views the agreement. The audit report also tracks when the email is viewed, unless this option is disabled. (Contact the Acrobat Sign support team if you wish to disable email tracking for your account.)
- Information about the file(s) used to create the agreement can be added in the audit report. This includes details such as the number of supporting files, the page count of the supporting files, and the names of the documents that contain signatures.

The audit report is associated to the signed document and is stored independently of the agreement objects viewed in the *Manage* page. The Sender and Internal Signers participating in the agreement can retrieve both the audit report and the associated signed document from the *Manage* page interface as two distinct PDF files. From the *Manage* page, it is also possible to retrieve the audit report concatenated with the agreement in one single PDF.

The signed document and the audit report are linked together through the Transaction ID of the agreement. This is a unique identifier assigned when the agreement is created. For enduring traceability, it is possible to print the Transaction ID along with the document name at the bottom of each page of the agreement PDF.

Optionally, settings can be configured to include a copy of the audit report and the associated signed PDF as attachments in the email sent to the participants once the agreement is final. Settings determine whether the email attachment is included for some or all recipients (Sender, Internal Signers, External Signers).

Learn more about audit reports here: https://helpx.adobe.com/sign/using/audit- reports-transaction-history.html

4.13 Audit Trail Capabilities *continued*

Hiding an object from the *Manage* page does not delete the audit report; the Transaction ID (if known) can be used to verify the audit report at any time.

The events captured in the audit report are also presented online in a dynamic Activity list for the agreement within the Acrobat Sign Solutions application. The Activity list is an element of the agreement and is destroyed by explicit actions that remove agreements. If the agreement is deleted, the history of activities is lost as well and cannot be recovered. An exception is possible if the agreement is deleted through system actions based on customer-defined retention rules that exclude deletion of the audit report. Refer to Managing Signed Records.

Considerations

In the scenario where an individual needs to apply multiple signatures in different signature fields within a single agreement, it is important to note that only one entry will be captured in the audit report to reflect the moment at which the Click to Sign button was actioned by the Signer for the set of signatures. If the user selected different reasons for signing in the distinct signature fields, each signing reason will be linked to a signature field and listed out individually in the audit report.

It is possible to route multiple documents for signature as part of a single agreement. By default, Acrobat Sign Solutions will merge the individual files before sending to the Signers. Through configuration, it is possible to separate the files once the agreement is completed. However, only one audit report will be generated for the agreement as a whole. If the intention is to obtain uniquely signed documents with their own audit report, the Sender should upload one document per agreement.

Refer to Managing Signed Records for considerations pertaining to the retrieval of signed documents and the associated audit reports from Acrobat Sign Solutions.

4.14 Date and Time Zone Settings

Overview

When applying electronic signatures, all date and timestamps are recorded using Adobe server time. The Adobe servers use the NTP Pool Project for time synchronization with known trusted external sources.

In the case of digital signatures, Public Key Infrastructure (PKI) creates a signature that is embedded in the document, using a digital certificate and a timestamp from the trust provider.

In the audit report, the date and time stamp format is set to YYYY-MM-DD - HH:mm:ss AM/PM [time zone], and this cannot be changed. The time zone code is supplied to provide context. The audit report shows all events standardized to the GMT time zone by default, and this is meant to take away confusion for auditors who are reviewing the audit report for agreements that were acted on across multiple time zones. However, it is possible to configure the *Global Settings* (at the account level) or *Group Settings* (at the group level) to use a different time zone for audit reports.

In the signature manifestation, the date and time stamp format reflect the recipient's local settings. The time zone code provides context and is displayed in signer's time zone (expressed in UTC with a time zone offset). If a different date format is preferred, an option is available to use a selected date format in electronic signature fields during the signing ceremony and in the signed PDF.

Considerations

The date and time formats in the audit report are set by Acrobat Sign Solutions and are not governed by configuration settings applied by the Customer. Configuration settings can only influence the format of the date in the signature manifestation. Therefore, it is important to ensure the date and time formats enforced by the Acrobat Sign Solutions service are acceptable according to internal policies for date and time recording.

4.15 Managing Signed Records

Overview

Once all signatures have been applied to a document using Acrobat Sign Solutions, all parties receive an email informing them that the signed record is available along with its audit report. It is possible to configure the email to include a hyperlink to view the signed record. The Sender and Internal Signers can access the signed record via the hyperlink (if included in the email) or directly from the Manage page in the Acrobat Sign Solutions interface. External Signers can access the signed record only via the hyperlink (if included in the email).

Content protection settings can be enabled for Internal and External Signers separately. When trying to view a protected agreement, the user will be challenged to authenticate before viewing the signed agreement. Signers will be prompted to authenticate using the same authentication method originally assigned to them on the agreement. When using content protection, no attachments will be included in emails sent by the system. This allows for increased security and follows best practices for accessing the signed agreements.

Learn more about content protection here: https://adobe.com/go/sign-config-content-protection

It is possible to configure the *Global Settings* (at the account level) or *Group Settings* (at the group level) so that a PDF copy of the signed record and its audit report are attached to the email sent to some or all participants (Sender, Internal Signers, and External Signers) at the completion of the agreement. While email provides convenient access to the signed document, the Customer should be mindful of any internal information protection and confidentiality policies that prohibit the routing of signed records via email.

Acrobat Sign Solutions encrypts documents and assets at rest and in transit. All Acrobat Sign Solutions documents are stored securely within the data layer (databases and file store) managed by Adobe. Backup management and recovery processes are routinely tested.

While Acrobat Sign Solutions is a safe repository for your agreements, it should not be used as a records management system. The signed record and its audit report can be retrieved for retention in an external system used by the Customer to manage the electronic records. This is possible either directly through the user interface or via API. Documents may be extracted from the Acrobat Sign Solutions interface as PDF files that are certified and sealed, providing proof of origin and integrity.

By default, all customer documents are retained on the Acrobat Sign Solutions service for as long as the Customer Account is active, provided that the size of that stored data does not exceed storage or technical limits set for the account. The data will not be deleted until the Customer takes explicit action to delete the agreements.

The Account Administrator can create retention rules by configuring *Data Governance* policies for their account. Retention rules define the timeframe after which agreements, transactions, and the supporting audit and personal information can be automatically deleted from the Acrobat Sign Solutions service.

When creating a retention rule, it is possible to define a distinct retention period for the agreement's activity log (audit trail). If this option is not enabled, only the documents, files and attachments that the Customer provided as part of the agreement will be deleted. Audit and personal information will not be deleted and the Transaction ID (if known) can still be used to verify that the agreement has taken place.

Learn more about data governance and retention here: https://adobe.com/go/adobesign_document_retention_guide

4.15 Managing Signed Records *continued*

Additionally, Acrobat Sign Solutions offers features to help Customers comply with the General Data Protection Regulation (GDPR). Users who are assigned top-level Privacy Administrator privileges have authority to view and delete the original agreement created by any user within their account after it has been determined to have served its designated purpose. A Privacy Administrator can irrevocably delete the original agreement from the Acrobat Sign Solutions service and the history of the agreement will be removed with the item. Customers should implement additional controls and procedures to manage the secure storage, distribution, and deletion of any copies of the agreement that are retrieved and maintained outside of Acrobat Sign Solutions.

Learn more about complying with GDPR requirements here: https://helpx.adobe.com/sign/admin/assets/gdpr-overview.html

Considerations

GxP business processes where Acrobat Sign Solutions will be used should include the retrieval of signed records and audit reports post-signature to ensure proper filing of the record and its audit report. Customers are accountable for their records and should implement procedural controls to ensure records are retrieved in a timely manner.

4.16 Sharing Accounts and Agreements

Overview

Acrobat Sign Solutions is designed to secure a user's content (agreements, templates, reports) from all other users, unless they are explicitly invited to view or interact with that content. In some organizational frameworks, it may be necessary to involve other individuals or roles (e.g. Line managers, Document Control team) to monitor the progress of an agreement without being an active participant (Sender or Signer) on the agreement. For these scenarios, different sharing options are available to allow users to expose their content.

The Account Sharing feature is available when the content of one user needs to be shared with any other user in the Customer's Account. This imparts a persistent view into the sharing user's agreements. With basic Account Sharing, the shared-with party gains view-only access to content in the sharing user's *Manage* page (In progress, Completed, and Canceled agreements and audit reports). With Advanced Account Sharing, the shared-with party will be able to view all content, modify in-process agreements, and send agreements on behalf of the sharing user.

Learn more about account sharing here: https://adobe.com/go/adobesign-share-accounts

When an individual needs to have visibility on a specific transaction but does not require a persistent view into the sharing user's entire list of agreements, the Agreement Sharing feature may be leveraged. Controls exist to allow sharing of agreements with Internal users only, External users only, or both. Sharing an agreement with another internal user will also populate the agreement on the shared-with user's *Manage* page, where they can review and monitor the agreement as it progresses. Upon sharing an agreement, the recipient receives an email with a PDF copy of the agreement in its current state. Once shared, it is possible to unshare the agreement. This will remove the agreement from the shared-with user's *Manage* page, but unsharing will not unsend the email with the attached PDF copy of the agreement. This issue may be avoided with the use of content protection controls. When content protection is enabled, attachments are not included in the emails and users must pass an authentication step before viewing a signed agreement.

Learn more about agreement sharing≈here: https://adobe.com/go/adobesign-share-agreement

Learn more about agreement unsharing here: https://adobe.com/go/adobesign-unshare-agreement

An alternative to Agreement Sharing is simply to include an individual's email address in the CC field when specifying the recipients of an agreement. The CC field can only be entered by the Sender when setting up the agreement.

Considerations

Sharing agreements should not be enabled unless the Customer defines appropriate sharing rules to safeguard the confidentiality and integrity of records from unauthorized access.

4.17 Signing Field Fillable FDA Forms

Overview

Some field fillable forms that are submitted to the FDA must be signed prior to submission (e.g. form number 1571, 1572, 0356h). Customers using and completing these forms should be aware that data security measures can remove business logic from the form once the form is uploaded to the Acrobat Sign Solutions service. This can present a challenge for the FDA, who require the form to remain 'live' as there are various teams at the agency that extract the data and text from the forms using different tools.

Considerations

If Customers find that the form has been 'flattened' after being processed through Acrobat Sign Solutions, FDA recommends submitting two copies of the form: (1) the completed and electronically signed form, and (2) the original and unsigned form that can be used as a working copy for data extraction.

Customers may opt to use Adobe Acrobat desktop applications (if available) to apply digital signatures on fillable FDA forms.

To clarify any uncertainties, Customers may contact the FDA directly.

4.18 PDF Certification

Overview

Acrobat Sign Solutions uses public key infrastructure (PKI) to certify signed documents and audit report PDFs. Certified PDFs can be easily recognized by a blue certification banner that prominently appears at the top of the PDF that is extracted from the system. This graphically displays a certification badge and affirms that the PDF is certified.

The default certification process seals the PDF and adds a permission password, preventing modifications to the files. This may pose a challenge for submissions to certain regulatory authorities who do not accept file level security. For Customers who require PDFs without security restrictions, the *Page Extraction* feature can be enabled to change the way the PDFs are sealed.

Learn more about the *Page Extraction* feature here: https://helpx.adobe.com/sign/config/security-settings/allow-page-extraction.html

When page extraction is enabled, the document is still sealed to preserve the integrity of the signatures while removing certain document restrictions such as content copying and commenting. Instead of displaying the certification badge, the blue certification banner at the top of the PDF only confirms that the document is signed.

Considerations

The *Page Extraction* feature is not exposed by default. Contact the Acrobat Sign support team if you wish to enable the feature for your account.

4.19 Signing Web Forms

Overview

Acrobat Sign Solutions offers the ability to create reusable web forms with fillable fields. Web forms can be embedded onto your website or shared via URL. The form can be viewed, filled out and signed by the participants.

Learn more about creating web forms here: https://helpx.adobe.com/sign/adv-user/web-form/create.html

Web forms respect the *Bio-Pharma Settings* to enforce the signer's identity authentication, allowing for signature compliance with 21 CFR Part 11 regulations. However, only the Acrobat Sign authentication and Phone authentication methods are supported for Signers.

Considerations

Web forms are particularly useful for establishing a self-service model, allowing individuals to retrieve and sign a document on their own without the delay of waiting for the agreement to be sent to them. However, since a web form is accessible via a public URL, anyone can access it. Enforced identity authentication can restrict access, but there is no identification verification process to confirm a person's identity. Appropriate procedural controls should be implemented to ensure that Signers have proven their identity and satisfied other organizational requirements.

Digital Signatures are not supported and should not be added when designing a web form.

4.20 Reporting

Overview

Users can leverage the dashboard on their *Reports* page to easily view agreement data. This data is represented graphically and can be refined with filters (e.g. date ranges, groups). A static snapshot of the data may be exported into a CSV file, facilitating further analysis of the data. There are numerous types of reports available. The number and types of reports available to users vary by the user's authority level and can be controlled at the user level.

Agreement reports present data related to productivity. The data is useful for understanding trends in agreement activity, such as agreement completion rates and average time to complete.

Transaction consumption reports present data related to account usage. This is useful for understanding transaction consumption patterns and who is using the system.

Settings Activity reports present a history of activity on account settings. Only administrators have access to this type of report. This is useful for analyzing when a user, group, or setting is changed and may be used to support periodic review activities.

Considerations

The New Reports experience will be enabled by default for all accounts, allowing Customers to experience the modern environment and gain the greatest benefits from the reporting capabilities.

5 How Adobe Helps Its Customers Achieve Compliance

5.1 Compliance with Industry Standards

Adobe understands that Healthcare and Life Science organizations have unique requirements and high-quality standards driven by regulations such as 21 CFR Part 11 and EudraLex Annex 11. As a cloud service provider, Adobe has implemented numerous processes and tools to support Customers in achieving their compliance goals.

Adobe Document Cloud - Acrobat Sign Solutions for enterprise and business are certified compliant with numerous certifications, standards, and regulations, such as ISO 27001, SOC 2 Type 2, PCI DSS, etc. Certifications and audit reports attest to the design, operation and effectiveness of controls adopted by Adobe. These certifications and audit reports are made available by Adobe so that Customers can leverage and review them as part of their vendor management and supplier assessment programs.

Visit the Adobe Trust Center to obtain access to copies of available certifications and audit reports. Some of these are only available under the terms of the non-disclosure agreement signed with Adobe. If required, the user will be prompted to electronically sign the non-disclosure agreement.

Learn more about security, privacy and compliance through the Adobe Trust Center here: https://www.adobe.com/trust.html

Consult the list of compliance standards and certifications relevant to Adobe Document Cloud here: https://www.adobe.com/trust/compliance/compliance-list.html

Adobe has established processes to support employees on their professional development paths. All employees are required to complete business code of conduct and security awareness trainings on a periodic basis. Additional training is offered to ensure that individuals responsible for the development and support of Adobe systems are qualified to perform their assigned tasks. Records of training completion are documented and retained.

5.2 Adobe Cloud and Infrastructure Control

Adobe maintains the Acrobat Sign Solutions service in a secure and controlled state. Infrastructure that supports the Acrobat Sign application undergoes strict controls and follows best practices for security, maintenance, and compliance. Lifecycle activities ensure that the infrastructure is designed and tested to verify that it can satisfy application requirements. Third parties to whom any infrastructure services are outsourced must undergo strict evaluation (per Adobe's vendor management program) prior to providing services to Adobe. Control processes are vetted by independent auditors who assess compliance with internationally recognized standards (ISO 27001, SOC 2 Type 2, and others) at a regular frequency.

5.3 Acrobat Sign Solutions Software Lifecycle

Acrobat Sign Solutions, the Acrobat Sign application, and their associated databases are developed and maintained according to a standardized software lifecycle management (SLC) process.

Adobe's SLC process includes a rigid quality testing phase. Test coverage includes common use cases, and testing must be completed successfully prior to releasing software updates. The following uses cases are included in Adobe's quality test plan for each release:

- **Send to Internal Signers** — Signature of a document by multiple Internal Signers (no External Signers)
- **Self-signing** — Signature of a document by a single Internal Signer who is also the Sender
- **Send to External Signers** — Signature of a document by one or more External Signers (no Internal Signers)
- **Send to both Internal and External Signers** — Signature of a document by Internal and External Signers

Refer to Appendix 1 for additional insight on these use cases.

Customers should evaluate the relevance of these use cases with respect to their intended use. Consideration should be given to avoiding unnecessary duplication of testing efforts by relying on Adobe's SLC process which implicitly tests and assures that these use cases can be completed in a consistent and reliable manner.

5.4 Service Commitments

Adobe service commitments describe Adobe's service availability for the Acrobat Sign Solutions services set forth in the sales order.

View all Adobe service commitments here: https://www.adobe.com/legal/service-commitments.html

Acrobat Sign Solutions' hosting environment leverages multiple cloud providers. Data is replicated across continuously active availability zones in multiple cloud regions. The landscape is designed to provide a high level of availability and scalability. Adobe continuously monitors Acrobat Sign Solutions, the Acrobat Sign service, and related infrastructure for performance.

Learn more about Adobe Acrobat Sign data centers here: https://helpx.adobe.com/sign/using/adobesign-data-centers.html

The data center configurations provide failover capability and resiliency. In the event of a data center disruption, traffic is routed to other data centers outside of the disrupted availability zone or to an entirely different cloud region.

View the availability status (uptime data) of the Acrobat Sign service here: https://status.adobe.com

Adobe deploys a comprehensive, ISO 22301-certified program for Business Continuity and Disaster Recovery. On an annual basis, Adobe conducts disaster recovery testing for Acrobat Sign Solutions to verify that cross-region failover and failback capabilities respect the stated recovery time and recovery point objectives. The disaster recovery plan is updated at least annually based on test results or following changes to the operating environment.

5.5 Security and Incident Response

As security threats are constantly evolving, a proactive security approach is followed. Adobe manages threat intelligence information and continuously monitors the Acrobat Sign Solutions service for the prevention and early detection of security vulnerabilities and incidents.

Adobe's security team conducts comprehensive and continuous security testing. The services of an outsourced third-party are retained to perform a security assessment and penetration testing covering network security, business logic, and web application security testing. Security testing reports are produced and published annually.

Adobe has implemented an incident response, mitigation, and resolution program. Each security incident is investigated and mitigated by Adobe's incident response team. Adobe personnel are required to complete security awareness training on an annual basis. Training content covers Adobe's current security policies and standards, and how to report security incidents to the response team.

Confirmed incidents are assigned a severity level based on impact, damage, or disruption to Customers. Adobe will notify customers of a confirmed Personal Data Breach in accordance with applicable law. Breach notification is addressed in the contractual terms between Adobe and the Customer.

Learn more about Adobe's security practices here: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/doc-cloud/acrobat-sign-security-overview.pdf

5.6 Release Management

Adobe maintains a well-defined process for managing, planning, testing, and scheduling releases of Acrobat Sign Solutions. Adobe plans to deliver three major feature releases each year. Major releases include new features and/or important changes to existing features. Minor release may be deployed at more frequent intervals to resolve customer-found defects or system processing issues as needed. Minor releases are not intended to introduce new features or changes that alter user experience, but there are exceptions. An Administrator can manage the risks associated with a release that introduces a new feature impacting the end user experience by enabling or disabling (as appropriate) the settings that control the feature's availability in the Customer Account.

Best efforts are made to release changes in the second week of the month. Planned launch dates are published on the Adobe Acrobat Sign Release Schedule.

The schedule outlines the tier of service that will be impacted by the change. The schedule also explains whether the feature will be standard (non-configurable) or configurable at the account or group-level in the Customer's Account.

Changes are planned and communicated by Adobe. All communications are produced specifically to provide information that Customers can use in their processes to manage change and the state of compliance. The following information is available:

- **Pre-release Notes:** Pre-release information is published for every major and minor release and is viewable on the Adobe Acrobat Sign Release Schedule page. It describes the scope of the release and highlights functional changes, enhancements and user interfaces updates. Pre-release information is published 8 weeks before, 4 weeks before, and again on the day of Production launch.
- **Technical Notifications:** These updates are typically long-term strategic changes that occur independently of the regularly scheduled major and minor releases. Usually, technical updates are planned and announced well in advance and commonly involve changes that relate to service deprecation.
- **Release Notes:** This document is published for every major and minor release. It is the final, refined version of the Pre-release notes. It highlights the new features, experience changes, and issues (bugs) resolved within the latest release. It is made available on the day of the release.

View Acrobat Sign Solutions release schedule and prerelease notes here: https://helpx.adobe.com/sign/release-notes/adobe-sign/sign-release-schedule.html

View Acrobat Sign Solutions technical notifications here: https://helpx.adobe.com/sign/using/technical-notifications.html

View Acrobat Sign Solutions release notes for the current release and previous releases here: https://helpx.adobe.com/sign/release-notes/adobe-sign.html

5.6 Release Management *continued*

Customers are encouraged to review the release documentation to gain visibility into functional or configuration changes. Customers are also encouraged to regularly review Acrobat Sign Solutions technical notifications to better understand Adobe's product roadmap and planned technical updates.

Customers should implement processes to ensure pre-release documentation and technical notifications are reviewed to assess upcoming changes and proactively plan for any perceived impact. In some cases, the changes may alter the business process use case. If system configuration changes are needed or the intended use of the system is affected, regression testing and/or re-validation activities may be required. Adobe will assist Customers with this assessment by publishing an assessment report which describes Adobe's evaluation of the potential impact of the upcoming changes from a regulatory compliance and validation perspective.

Customers who take intentional action to activate or disable new features should follow established management procedures before changing any settings in the Customer Account.

5.7 Adobe Acrobat Sign Sandbox

Enterprise-tier customers can subscribe to the Adobe Acrobat Sign Sandbox. This environment is discrete from the production environment. Agreements sent from Sandbox will be watermarked as "Not for production use".

The purpose of Sandbox is to allow administrators to define, modify, and test setting configurations as desired without having any effect on production activities. Sandbox is delivered as a clean environment with default configuration and does not mirror the Customer's production settings. However, to facilitate the synchronization of the two environments, an administrator can copy some setup (such as group names, library templates, custom workflows) to and from the production environment.

The account or group level settings in Sandbox generally match the setting options that are found in the production environment, with the exception of any new/updated settings that are pending release. The Sandbox environment is updated with new content 4 weeks before a major launch in production. While this means that the two environments will be misaligned for 4 weeks, it provides the benefit of being able to assess and test new features that are approaching release before landing in production.

Customers should also be aware of fully disclosed feature differences between Sandbox and the production environment (e.g., such as suppression of outbound emails, integrations not available with Sandbox accounts). The scope of this paper is to discuss Sandbox environment for the core Acrobat Sign application only and not for system integration with other solutions.

Learn more about the Adobe Acrobat Sandbox offering here: https://helpx.adobe.com/sign/using/adobesign-sandbox.html

5.8 Validation Support

If using Acrobat Sign Solutions to apply electronic signatures in an GxP-regulated context, Customers are responsible for validating Acrobat Sign Solutions to demonstrate (with objective evidence) fitness for their intended use and that the system functions in a consistent and reliable manner and offers the ability to discern altered or invalid records/ signatures.

Customers should establish the appropriate level and extent of validation. Regulatory agencies and industry best practices, such as ISPE's GAMP 5 (Ref. [3]), recommend following a risk-based approach to validation. Leveraging supplier activities is encouraged to make the validation effort as effective and efficient as possible.

Adobe offers validation document templates to assist Customers in their validation efforts. While the template package covers a set of typical use cases, other use cases are possible but not considered in the package. The use cases that are covered in the validation document template package pertain to the core Acrobat Sign web application only and do not cover the mobile application nor address use cases involving system integration with other solutions. The Customer has the responsibility of assessing the suitability of the templates (including use case coverage) and may choose to adapt and execute these validation documents to establish documented evidence that their instance of Acrobat Sign Solutions is fit for intended use. These documents are updated and re-issued as necessary for each major release, in conjunction with an impact assessment report which describes the potential impact from a validation perspective.

Learn more about the validation document template package here: https://helpx.adobe.com/sign/using/21-cfr-validation-pack.html

Customers who qualify for a Sandbox environment may consider setting up an instance as a controlled environment that can be used for pre-production and validation testing purposes.

5.9 Customer Care

Customers may consult the online Adobe Help Center any time for answers to frequentlyasked questions (FAQ), user guides and tutorials.

View the Acrobat Sign help center here: https://helpx.adobe.com/support/sign.html

For personalized assistance, Acrobat Sign Solutions customers can submit a case to Adobe Support. Only administrators have the authority to submit support cases. Customers can contact Adobe Support to report issues observed in their Acrobat Sign Sandbox and Production instances.

Customers can also contact Adobe Support to request changes to settings that are not customer-facing through the application interface. However, when doing so, the customer should implement processes (such as change and configuration management) to track the request and the impact of the settings change on their end.

6 Implementing Acrobat Sign Solutions — A Practical Guide

6.1 Implementation Checklist

Follow this step-by-step list of actions to get a Customer Account up and running with Acrobat Sign Solutions.

Step	Activity	Actions	Configuration
1.	Identification of business use cases: Intended Use	Examine your business processes to establish what type of documents will need to be signed using the Acrobat Sign service and by whom.	N/A
2.	Account creation	Read Getting Started. Acrobat Sign Solutions, enterprise or business levels of service, is required to benefit from Bio-Pharma settings and other advanced features. An enterprise plan is needed if implementing Acrobat Sign with Single Sign On (SSO) or if a subscription to Sandbox is desired. Adobe services will support on-boarding the account and provide access to the Adobe Admin Console. Create a user appointed as the Acrobat Sign Solutions Account Administrator.	N/A
3.	Group management	Read Setting up the Account with Groups. As the Account Administrator, create group(s) for users that will be subject to controls of Bio-Pharma Settings (i.e. GxP group) and separate groups for those that will not need to sign in regulated environments (i.e. non-GxP group). Designate user(s) who will act as group administrator for the GxP group. Allow group administrators to add users and edit settings for their group. As the Group Administrator, configure additional settings for the business process.	Account>GlobalSettings > Groups Account > Groups > Group Settings
4.	Type of signature	Read Signature Types. If opting for electronic signatures: As the Group Administrator, configure the GxP group to allow electronic signatures. If opting for certificate-based digital signatures: As the Group Administrator, configure the GxP group to allow digital signatures. Choose and on-board a trust service provider (TSP) and distribute signing instructions for use with digital IDs.	Account > Groups > Signature Preferences Account > Groups > Digital Signatures

6.1 Implementation Checklist *continued*

Step	Activity	Actions	Configuration
5.	Authentication settings	Read Identity Authentication Methods for Electronic Signatures. As the Group Administrator, configure authentication methods for the GxP group: • For Internal Signers: Select Acrobat Sign authentication. • For External Signers: Select Acrobat Sign authentication, Phone authentication, One Time Password via Email	Account > Groups > Send Settings
6.	Single Sign-On	Read Using Single Sign-On (SSO) for User Authentication. As an administrator in the Adobe Admin Console, configure the account to use Federated IDs (if desired). As the Account Administrator, enable single sign-on (if desired).	Adobe Admin Console Or Account > Account Settings > SAML Settings
7.	Allow External Signers	Read Implications for External Signers. As the Group Administrator, configure the GxP group to allow External Signers to participate in signature agreements. Implement a process so Senders can identify allowed Signers.	Account > Groups > Signature Preferences Account > Groups > Send Settings
8.	Authorization	Read Adding Users to the Account and Groups and read Apply and Manage User Permissions. Implement a process for user access management. Create users manually or through synchronization with the organization's enterprise directory. As an administrator in the Adobe Admin Console, assign user entitlement to the Acrobat Sign Solutions product. As the Account Administrator or the Group Administrator, place users in the GxP group. As the Account Administrator or the Group Administrator, assign the user's authority level (user permissions).	Account > Users
9.	Bio-Pharma Settings	Read Bio-Pharma Settings to Support 21 CFR Part 11 Requirements and read Bio-Pharma Settings to Configure the Signature Manifestation. As the Group Administrator, enable and configure Bio-Pharma Settings for the GxP group. As the Group Administrator, configure the pre-defined list of reasons for signing (excluding the blank reason).	Account > Groups > Bio-Pharma Settings

6.1 Implementation Checklist *continued*

Step	Activity	Actions	Configuration
10.	Date and time	Read Date and Time Zone Settings. As the Group Administrator, configure the preferred date and time zone settings for the GxP group.	Account > Groups > Group Settings
11.	Optional features	Read Signature Delegation, Sharing Accounts and Agreements, PDF Certification and Signing Web Forms. As the Group Administrator, configure additional features as required to fit business process requirements.	Account > Groups > Group Settings Account > Groups > Security Settings

7 Governance

7 Governance

As with any system that must comply with 21 CFR Part 11 and EudraLex Annex 11 requirements, Customers must employ procedures and controls to ensure the integrity of electronic records and electronic signatures. Customers should review their internal policies and procedures to ensure the intended use of Acrobat Sign Solutions is aligned with their needs.

The following table highlights some of the key governance processes which need to be implemented by the Customer to support the use of Acrobat Sign Solutions, along with some recommendations and considerations.

Topic	Consideration
System Administration	Define roles and responsibilities for reviewing the Adobe roadmap and technical update documentation prior to each release. Adobe produces documentation on the changes to their service prior to every major and minor release. Pre-release notes and other notifications about the status of the Acrobat Sign Solutions service should be reviewed to evaluate upcoming functional changes and, if necessary, appropriate action taken.
User Access Management	Define the process for creating user accounts and granting the correct level of permissions based on the users' roles and responsibilities. User account management can be integrated with the existing identity provider (i.e. automated user creation) or through a manual user creation process.
Use of Electronic Signatures	Define internal policies that hold individuals accountable and responsible for actions initiated under their electronic signatures. These policies should be designed to deter signature falsification. The consequences of inappropriate use of electronic signatures should be clarified. Define the process for the application of electronic signatures to electronic records in compliance with US FDA 21 CFR Part 11 and (if needed) EudraLex Volume 4 Annex 11 requirements. The process should emphasize authentication requirements for the key regulated use cases. However, the broader use of electronic signatures may not need these controls. Determining signature use cases is critical to successful rollout.
Records Management	Define the process for extracting signed electronic records and their audit trails (audit reports) from Acrobat Sign Solutions and into the designated electronic records repository or archive that is managed by the Customer.

In addition to the procedures outlined above, Customers are reminded that policies, procedures, or other quality system documents should be implemented to address the following topics to ensure Acrobat Sign Solutions is validated, implemented, managed, and used in a controlled fashion:

- Computer System Validation
- Logical Security
- Training Management
- Documentation Management
- Change and Configuration Management
- Backup and Recovery
- Disaster Recovery and Contingency Planning
- Periodic Review
- Vendor Assessment
- Incident and Problem Management

8 Appendix 1: Overview of Business Use Cases

8 Overview of Business Use Cases

Common business use cases are presented below to illustrate how the Customer can implement Acrobat Sign Solutions for the application of 21 CFR Part 11 and Annex 11 compliant electronic signatures.

Description of Use Case	Example(s)	Insight
Send to Internal Signers	• Approving a validation artifact (Validation Plan, Validation Protocol, etc.) • Approving a standard operating procedure (SOP)	The *Send* page interface is used to send an agreement to internal recipients. The Sender may or may not be one of the Signers.
Self-signing	• Signing a Note to File or other form/ report by the individual issuing the document where additional approvals are not required • Signing an Incident report • Signing your own status report	This use case pertains to the signature of a document by a single Internal Signer who is also the Sender. The Signer will click the *Fill and Sign a documen*t tile to signer the agreement themselves (self-signing). The Signer can also use the *Send* page interface to send an agreement to themselves (self-sending)
Send to External Signers	• Signing a waiver • Signing an informed consent form • Signing a contract with supplier	The *Send* page interface is used to send an agreement to one or more signers that are not members of the customer's account.
Send to both Internal and External Signers	• Signing a controlled document (e.g., SOP, validation deliverable, etc.) where one or more of the Signers are consultants or contractors who have not been added to the organization's Acrobat Sign Solutions account. • Site Contracts for clinical studies which are signed by the sponsor (internal) and the investigator (external)	The *Send* page interface is used to send an agreement that either the Sender or another internal team member will sign prior to or after an external signer. The Sender may or may not be one of the Signers.

9 References

9 References

Ref. [1] U.S. Food and Drug Administration, Code of Federal Regulations, Title 21 Part 11, *Electronic Records; Electronic Signatures,* 1997.

Ref. [2] EudraLex, The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medical Products for Human and Veterinary Use, *Annex 11: Computerised Systems,* 2011.

Ref. [3] ISPE, GAMP 5 - *A Risk-Based Approach to Compliant GxP Computerized Systems*, Second edition, 2022.

10 Acknowledgment

10 Acknowledgment

This document was prepared through a collaboration between Adobe and Montrium Inc.
Learn about Montrium at www.montrium.com.

This document is geared towards Healthcare and Life Science organizations who are FDA-regulated and/or operating within the European Union. This document is meant as a reference for making independent decisions regarding the use of Acrobat Sign Solutions. This document does not constitute legal or professional advice. Organizations should perform adequate diligence based on their internal processes to ensure Acrobat Sign Solutions align with their intended use. Laws and regulations change frequently, and this information may not be current or accurate. To the maximum extent permitted by law, Adobe provides this material on an "as-is" basis. Adobe disclaims and makes no representation or warranty of any kind with respect to this material, express, implied or statutory, including representations, guarantees or warranties of merchantability, fitness for a particular purpose, or accuracy.


Adobe