Présentation technique d'Adobe Sign

Sécurité, conformité, gestion des identités, gouvernance et gestion des documents

Sommaire

Résumé

Solution Document Cloud, *Adobe Sign* aide votre entreprise à déployer des expériences digitales complètes, axées sur les documents et assorties de signatures électroniques légales et fiables. Faites appel à Adobe Sign pour faciliter la diffusion, la signature, le suivi, la gestion et l'archivage de documents numériques à partir d'applications web ou mobiles — ou de systèmes d'entreprise. Conforme à nombre de réglementations et normes sectorielles, Adobe Sign est accessible partout, sur tout type d'équipement. Ce service cloud très robuste gère en toute sécurité un grand nombre de processus de *signature électronique* :

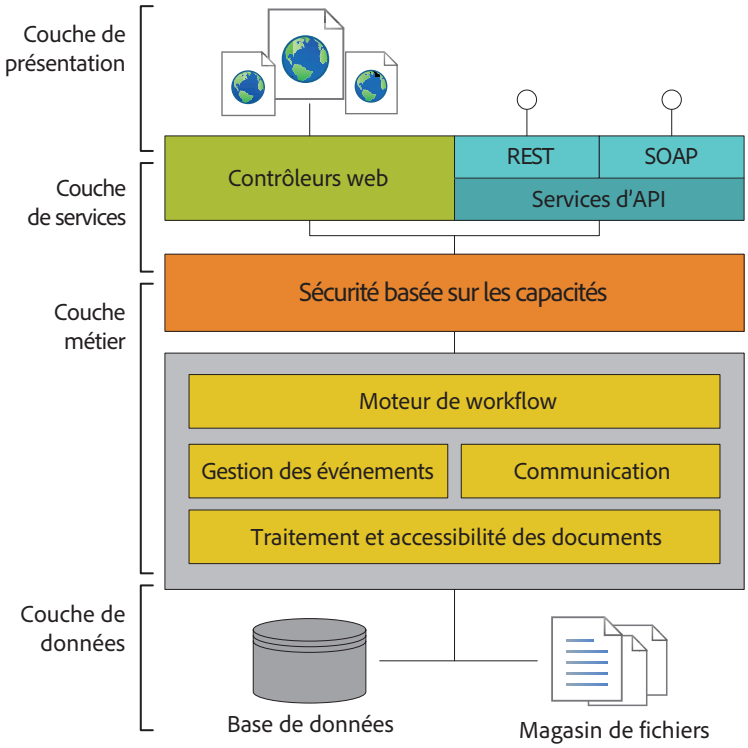
- Gestion des identités des utilisateurs avec authentification basée sur les capacités
- Certification de l'intégrité des documents
- Vérification des signatures électroniques
- Journalisation de l'acceptation du destinataire ou de la réception des documents.
- Gestion de pistes d'audit
- Intégration dans vos applications métier et systèmes d'entreprise stratégiques.

Adobe Sign prend en charge les signatures électroniques et *numériques*. La signature électronique est un moyen de signifier son accord ou sa validation sur un document ou un formulaire numérique. Les signatures électroniques ont force exécutoire et sont juridiquement recevables dans de nombreux pays industrialisés. Une signature numérique est une implémentation spécifique d'une signature électronique qui utilise un identifiant numérique basé sur un certificat pour vérifier l'identité du signataire et lier la signature au document par un cryptage. Adobe Sign est compatible avec les identifiants numériques enregistrés dans les cartes à puce, les jetons USB et les modules HSM basés dans le cloud. En outre, il prend en charge le standard de signature ouvert avec les identifiants numériques sur les postes de travail, le web et les terminaux mobiles à l'aide de la spécification du Cloud Signature Consortium.

Cet article technique fournit une présentation générale de l'architecture, de la sécurité, de la conformité, de la gestion des identités, de la gestion des documents, de la protection du réseau, du suivi des performances, de la gestion des services, de la gouvernance et d'autres aspects techniques clés d'Adobe Sign. Pour en savoir plus sur l'utilisation des différents types de signature, consultez l'article technique d'Adobe intitulé *Transformer les processus métier grâce aux solutions de signature électronique et numérique*.

Architecture

L'architecture d'Adobe Sign est conçue pour évoluer et gérer de gros volumes de transactions sans aucune détérioration des performances. Pour garantir un niveau élevé de disponibilité et d'évolutivité, toutes les données transactionnelles d'Adobe Sign sont stockées dans plusieurs clusters de bases de données redondantes distribuées, avec basculement et restauration automatiques[1]. Le schéma de l'architecture multicouche ci-dessous illustre la répartition logique des composants et fonctionnalités d'Adobe Sign :



Architecture logique d'Adobe Sign

Chaque couche logique de l'application Adobe Sign est surveillée par une suite complète d'outils qui suivent des indicateurs clés, tels que le temps moyen de conversion des documents au format PDF ou l'utilisation des ressources. Le tableau de bord de surveillance permet aux ingénieurs chargés des opérations Adobe Sign de visualiser facilement l'état général du service. Si l'un des indicateurs clés dépasse le seuil de surveillance défini, les ingénieurs chargés des opérations en sont informés par des notifications en temps réel. Si un problème ne peut être évité, Adobe Sign tient des journaux complets de diagnostic et d'analyse qui aident les ingénieurs à le résoudre rapidement et à traiter la cause première afin qu'il ne se reproduise pas.

Couche de présentation

La couche de présentation gère l'interface utilisateur web, ainsi que la génération, l'affichage et le rendu des documents pour signature, des fichiers PDF certifiés finaux et des composants du workflow.

Couche de services

La couche de services gère les fonctions de contrôle requises pour les API des services client et web, telles que la passerelle REST et l'API SOAP. Les serveurs web des systèmes tournés vers l'extérieur gèrent les requêtes des navigateurs et des API, et les serveurs de messagerie le trafic des communications entrantes et sortantes. Les serveurs web distribuent les requêtes dynamiques complexes aux serveurs d'applications Adobe Sign dans la couche métier en utilisant des équilibreurs de charge. Les serveurs web de la couche de services intègrent également des règles de filtrage de sécurité pour empêcher les attaques web courantes ainsi qu'un pare-feu pour renforcer le contrôle des accès.

[1] La reprise automatique se limite à l'infrastructure Amazon Web Services.

Couche métier

La couche métier d'Adobe Sign gère le workflow, la sécurité basée sur les capacités, les services de conversion de documents et d'imagerie, les événements, la journalisation et la surveillance, la consultation et l'utilisation des fichiers, ainsi que les fonctions de communication.

Moteur de workflow

Le moteur de workflow d'Adobe Sign exécute et gère l'ensemble des processus métier, ainsi que les étapes du processus de signature d'un document. Il utilise un langage de définition XML déclaratif pour décrire les conditions préalables à l'exécution de flux propres aux clients et la séquence d'événements requise pour mener à bien un processus de signature ou d'approbation.

Sécurité basée sur les capacités

La sécurité basée sur les capacités d'Adobe Sign gère la définition, le contrôle et l'audit des ressources disponibles et des opérations autorisées par un utilisateur ou une application authentifié sur ces ressources. Les ressources englobent toutes les informations sous forme de documents, de données, de métadonnées, d'informations sur les utilisateurs, de rapports et d'API.

Gestion des événements

La gestion des événements d'Adobe Sign enregistre et conserve une piste d'audit pour les informations pertinentes sur chaque utilisateur et document. À chaque étape du workflow, Adobe Sign génère un événement et — via un système de messagerie asynchrone — distribue des messages aux ressources système appropriées.

Communication

Adobe Sign utilise la messagerie électronique pour l'envoi des notifications d'événement de signature et la distribution facultative des documents signés et certifiés à la fin du processus. Pour limiter le spam et le phishing, Adobe Sign permet d'authentifier les e-mails avec les fonctionnalités Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) et Sender Policy Framework (SPF).

Traitement et consultation des documents

Pour améliorer les performances, le moteur de traitement des documents d'Adobe Sign offre une fonctionnalité sans état pour convertir différents formats de fichiers en documents PDF, crypter et décrypter des fichiers, et pixelliser des images pour affichage dans un navigateur web. Adobe Sign exécute des opérations de traitement documentaire à l'aide d'un système de messagerie asynchrone basé sur une file d'attente pour les communications entre les ressources système. Par ailleurs, le traitement des documents et l'accès au stockage NAS s'exécutant en arrière-plan, les processus Adobe Sign paraissent instantanés à chaque étape du workflow.

Couche de données

La couche de données gère l'accès à la base de données transactionnelles, à la base de données du système de messagerie asynchrone et au magasin de documents. Au nombre des données transactionnelles stockées dans la couche d'accès aux données figurent le document original du client, les versions intermédiaires du document générées durant le processus de signature, les métadonnées du document, les utilisateurs, les événements et le document PDF final signé et traité par Adobe Sign.

Intégrations

Adobe Sign permet des intégrations clés en main avec une multitude d'applications métier et de systèmes d'entreprise, tels que Salesforce, Apttus, Workday et Ariba, sans oublier les solutions Microsoft comme SharePoint, Dynamics et les applications Office. Cette solution offre également un jeu complet d'API pour personnaliser l'intégration avec des systèmes métier propriétaires ou des sites web d'entreprise via des services web HTTPS, SOAP ou REST sécurisés. Pour obtenir la liste des intégrations prises en charge par Adobe Sign, reportez-vous à la *page de présentation des intégrations*.

Gestion d'identités

Pour la gestion des identités, Adobe Sign utilise un modèle basé sur les rôles qui gère l'authentification, l'autorisation et le contrôle d'accès dans tout le système Adobe Sign. Des processus de sécurité et d'authentification basés sur les capacités sont définis et activés pour une structure donnée par un administrateur Adobe Sign. Adobe Sign définit les rôles d'utilisateur suivants :

- **Expéditeur** — Utilisateur titulaire d'une licence qui a reçu des autorisations Adobe Sign d'un administrateur pour créer des workflows de signature et envoyer des documents pour signature, approbation ou consultation.
- **Signataire** — Utilisateur vérifié auquel un expéditeur a fourni un accès pour signer un document particulier. Par défaut, Adobe Sign envoie au signataire un e-mail contenant une URL unique vers le document à signer, qui est constituée d'identifiants exclusifs et propres à la transaction.
- **Approbateur** — Utilisateur vérifié auquel un expéditeur a fourni un accès pour approuver un document.
- **Autre** — Utilisateur vérifié auquel un expéditeur a fourni un accès pour consulter un document ou une piste d'audit.

Authentification des utilisateurs

Adobe Sign utilise plusieurs méthodes pour authentifier un utilisateur, y compris l'authentification à un et plusieurs facteurs, ainsi que des options supplémentaires. En général, un utilisateur titulaire d'une licence se connecte à Adobe Sign avec une adresse e-mail et un mot de passe vérifiés qui correspondent à une identité authentifiée telle qu'un Adobe ID. Les administrateurs peuvent également configurer la sécurité et la complexité du mot de passe, la fréquence du changement, la comparaison avec l'ancien mot de passe et les politiques de verrouillage (telles que l'expiration du renouvellement de connexion).

L'authentification classique sur Adobe Sign consiste à envoyer une demande par e-mail à une personne bien précise. Il s'agit là du premier niveau d'authentification, sachant que la plupart des utilisateurs disposent d'un accès exclusif à un compte de messagerie. Le premier niveau d'authentification est souvent utilisé pour le signataire, l'approbateur ou d'autres types d'utilisateurs. Pour renforcer la sécurité et empêcher les usurpations d'identité par des individus malveillants, il est également possible d'ajouter des méthodes d'authentification à plusieurs facteurs, comme l'authentification par téléphone, par SMS ou basée sur les connaissances (KBA), en fonction de leur disponibilité dans votre zone géographique.

Adobe Sign prend en charge les types d'authentification suivants :

- **Adobe Sign ID** — Combinaison d'une adresse e-mail et d'un mot de passe vérifiés, utilisée par un utilisateur titulaire d'une licence pour se connecter en toute sécurité à un compte Adobe Sign.
- **Adobe ID** — L'Adobe ID donne accès à tous les services Adobe sous licence, y compris Adobe Sign. Adobe surveille en permanence les comptes Adobe ID afin de détecter d'éventuelles activités inhabituelles ou anormales, et de limiter rapidement les menaces de sécurité potentielles.
- **Google ID** — Identification d'utilisateur authentifiée par Google (par exemple, Gmail or G Suite).
- **Authentification unique (SSO)** — Les entreprises à la recherche d'un mécanisme de contrôle d'accès plus strict peuvent activer l'authentification unique SAML (Security Assertion Markup Language) afin de gérer les utilisateurs Adobe Sign avec leur propre système d'identification. Adobe Sign peut également être configuré de façon à reconnaître et intégrer les principaux fournisseurs spécialisés dans la gestion des identités, comme Okta et OneLogin.

Certification des documents

À chaque étape du workflow, Adobe Sign utilise une somme de contrôle sécurisée pour garantir l'intégrité et la confidentialité du document. Il se base sur une infrastructure à clé publique (PKI) pour certifier les documents PDF finaux avec une signature numérique avant de les distribuer à tous les participants.

La signature numérique est créée avec un algorithme de hachage qui extrait des informations uniques du document PDF final signé afin de générer une chaîne de chiffres et de lettres à codage hexadécimal cryptographiquement correcte et de longueur fixe. Affichée sous forme de bannière bleue et de badge de certification en haut du PDF final signé, la signature numérique vérifie l'intégrité du document (voir la figure suivante) et garantit qu'il n'a pas été falsifié depuis la délivrance du certificat. Si nécessaire, la sécurité du PDF certifié final peut être renforcée par un mot de passe.

Version Acrobat DC — badge noir

Acrobat X et XI — badge bleu (versions 10 et 11)

Bannières et badges de certification des documents Adobe Sign

Pour générer les clés de verrouillage et de certification du PDF final signé, Adobe Sign utilise des certificats délivrés par des autorités de certification et services d'horodatage de confiance. Dans certains cas, Adobe Sign peut être configuré de façon à émettre des documents certifiés par les autorités de certification des gouvernements, par exemple en Suisse, au Brésil et en Inde. Les clés PKI utilisées pour certifier le PDF final sont stockées dans un module de sécurité matériel pour empêcher les attaques et les falsifications en ligne.

Sécurité

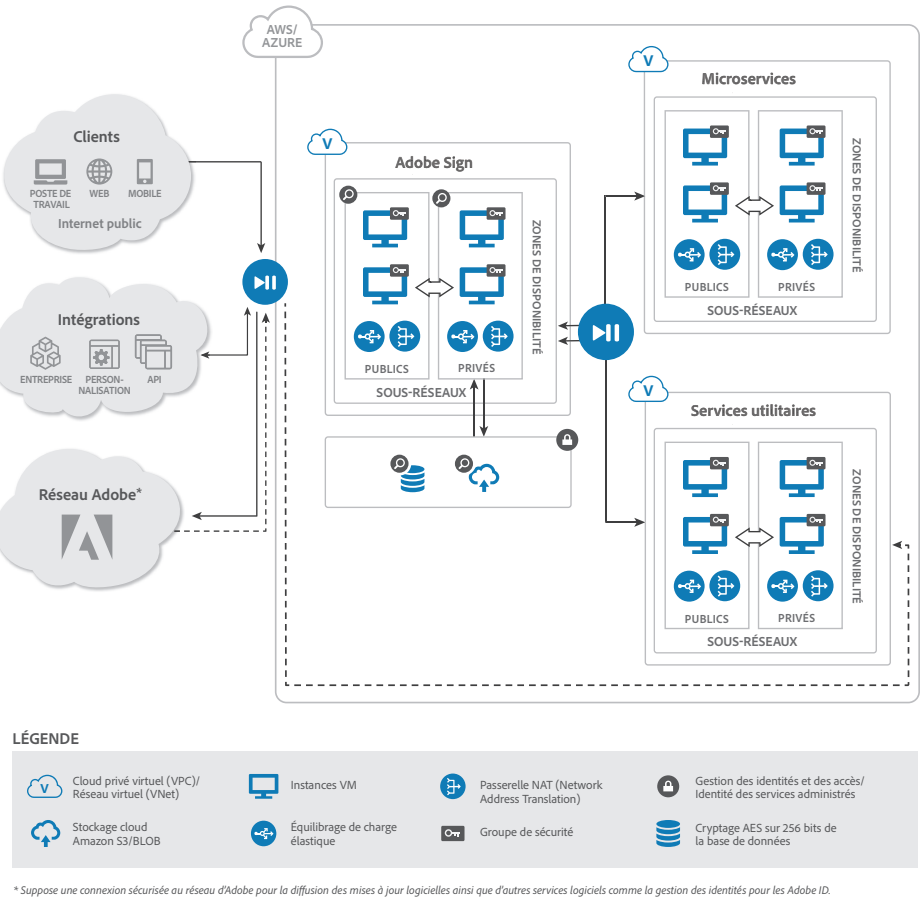
Les pratiques de sécurité et mesures de protection de la vie privée sont profondément ancrées dans la culture d'Adobe, ainsi que dans ses processus de développement logiciel et d'opérations de service. Adobe Sign applique des pratiques de sécurité standard — pour la gestion des identités, la confidentialité des données et l'intégrité des documents — afin d'optimiser la protection de vos documents, données et informations personnelles. L'infrastructure d'Adobe Sign réside dans des centres de données ANSI (American National Standards Institute) de niveau 4 gérés par nos fournisseurs de services cloud de confiance, AWS (Amazon Web Services) et Microsoft Azure.[2] Tous les partenaires d'hébergement de l'infrastructure d'Adobe Sign contrôlent de façon très stricte l'accès aux centres de données, la tolérance aux pannes, les paramètres environnementaux et la sécurité réseau. Seuls les employés approuvés et habilités d'Adobe, les employés des fournisseurs de services cloud et les sous-traitants exerçant une activité légitime et documentée sont autorisés à accéder aux sites sécurisés en Amérique du Nord, au Japon, en Australie, en Inde et dans l'Union européenne.

Dans le cadre de son engagement en faveur de la sécurité, Adobe examine régulièrement les attestations de conformité telles que les rapports SOC 2 Type 2 et ISO 27001, et surveille activement tous les composants d'Adobe Sign au moyen de systèmes standard de détection et de prévention des intrusions. Pour en savoir plus sur les processus de sécurité d'Adobe, l'engagement communautaire et Adobe SPLC (Secure Product LifeCycle), consultez le site *www.adobe.com/fr/security*.

[2] Disponibilité prévue au troisième trimestre 2018.

Architecture de sécurité réseau

La vue d'ensemble de la topologie réseau ci-après représente l'architecture de sécurité d'Adobe Sign, notamment les serveurs externes, les serveurs cloud et les accès clients.



** Suppose une connexion sécurisée au réseau d'Adobe pour la diffusion des mises à jour logicielles ainsi que d'autres services logiciels comme la gestion des identités pour les Adobe ID.*

Serveurs externes

L'architecture réseau hébergée des services Adobe Sign comprend des systèmes tournés vers l'extérieur, notamment des *serveurs web* pour gérer les requêtes des navigateurs et des API, et des *serveurs de messagerie* qui se chargent du trafic des courriers électroniques entrants et sortants. S'appuyant sur des équilibreurs de charge matériels, les serveurs web sont chargés de distribuer les requêtes dynamiques complexes aux serveurs d'applications. Ils intègrent des règles de filtrage de sécurité pour esquiver les attaques web courantes ainsi qu'un pare-feu pour assurer un contrôle robuste des accès.

Réseaux cloud virtualisés

L'architecture de sécurité réseau d'Adobe Sign repose également sur plusieurs réseaux cloud virtualisés. Dans l'environnement AWS, ceux-ci sont appelés cloud privé virtuel (VPC), et Microsoft Azure utilise l'appellation réseau virtuel (VNet). Un VPC/VNet est un réseau isolé logiquement, séparé des autres instances d'Adobe Sign et inaccessible depuis celles-ci. Chaque VPC/VNet est composé de sous-réseaux, englobant diverses adresses IP. Les sous-réseaux peuvent être publics ou privés. Un sous-réseau public est relié à Internet, contrairement au sous-réseau privé. Les caractéristiques des VPC/VNet utilisés par le service Adobe Sign sont les suivantes :

- Les réseaux VPC/VNet privés et publics sont chargés des processus métier du service Adobe Sign. La logique applicative d'Adobe Sign est gérée par un sous-réseau privé s'exécutant sur des serveurs cloud virtuels sécurisés et évolutifs qui sont uniquement accessibles via des connexions émanant du sous-réseau public.
- Les VPC/VNet des microservices s'appuient sur une architecture compartimentée, à base de conteneurs, afin de faire place à des services s'exécutant « en milieu clos », ultra-évolutifs et performants, n'ayant aucune incidence sur l'infrastructure système sous-jacente. Adobe Sign fait appel aux microservices pour des actions spécifiques, comme l'intégration de signatures numériques avec le CSC (Cloud Signature Consortium), la validation de signatures et la suppression de l'arrière-plan des images de signatures.
- Les VPC/VNet des services utilitaires gèrent la surveillance et la journalisation des événements ainsi que les référentiels de réplication des artefacts de service.

Sous l'angle de l'architecture réseau, une zone de disponibilité (AZ) réside au sein d'une instance VPC/VNet. Physiquement, chacune de ces zones comprend plusieurs centres de données redondants différents. Toutes les données sont répliquées entre la totalité des centres de données, et entre plusieurs serveurs au sein de chaque centre.

Les instances VPC/VNet sont verrouillées dans un groupe de sécurité. À l'instar d'un pare-feu virtuel, les groupes de sécurité permettent à Adobe de renforcer le contrôle du trafic entrant et sortant en direction de l'instance VPC/VNet. Adobe a ainsi la certitude que seuls les utilisateurs légitimes exécutent des actions autorisées. De plus, l'architecture de sécurité réseau d'Adobe Sign comprend des capteurs de protection/détection des intrusions positionnés à des emplacements clés pour garantir l'intégrité des systèmes et une visibilité à l'échelle du service.

Accès clients

Le service Adobe Sign est accessible à partir de divers points d'accès clients, tels un navigateur, une application mobile ou par e-mail. Lorsqu'un client se connecte à Adobe Sign dans sa région, il passe par une passerelle Internet donnant accès à plusieurs VPC/VNet. Toutes les connexions clientes sont opérées via le protocole HTTPS utilisant TLS1.2 (à compter de juin 2018) avec un cryptage AES sur 128 bits au minimum.

Protection du réseau

Tous les fournisseurs de services Adobe Sign utilisent des équipements réseau pour contrôler les communications qui transitent à l'intérieur et à l'extérieur du périmètre du réseau. Ces pare-feu et autres systèmes de protection exploitent des jeux de règles, des listes de contrôle d'accès (ACL) et des configurations pour acheminer les informations vers certains systèmes informatiques. Des listes ACL ou règles de trafic sont présentes sur chaque interface gérée pour assurer et gérer le trafic, et sont tenues à jour par des processus automatisés.

Les deux fournisseurs font également appel à divers systèmes de surveillance automatisés pour garantir un haut niveau de performance et de disponibilité. Les outils de contrôle servent à détecter les activités inhabituelles ou non autorisées aux points d'entrée et de sortie du réseau afin de remédier aux failles de sécurité classiques :

- Attaques DDoS (Distributed Denial Of Service)
- Attaques MITM (Man in the Middle)
- Usurpation d'adresse IP
- Balayage de ports
- Reniflage de paquets par d'autres locataires

Adobe utilise les protocoles SSH (Secure Shell) et SSL (Secure Sockets Layer) pour instaurer des connexions sécurisées permettant de gérer les connexions à l'infrastructure hébergée des services Document Cloud.

Cryptage

Adobe Sign exploite uniquement des *algorithmes de cryptage conformes à la norme PCI DSS* pour sécuriser les documents et ressources stockés à l'aide d'un cryptage AES 256 bits, et prend en charge HTTPS TLS v1.2 (ainsi que certaines versions antérieures) pour veiller à ce que les données transmises soient également protégées. Les documents en question sont sécurisés dans des containers de stockage cryptés, qui sont uniquement accessibles avec les autorisations de sécurité basées sur les capacités appropriées via la couche d'accès aux données applicatives sur un sous-réseau privé. De plus, les expéditeurs peuvent également renforcer la sécurité d'un document en utilisant un mot de passe privé.

Les clés de cryptage de document sont stockées dans un environnement sécurisé avec des restrictions d'accès et une rotation, si nécessaire, dans le respect des règles Adobe de gestion des clés. Un hébergeur fiable recourt à un chiffrement fort à plusieurs facteurs ; il crypte notamment chaque objet avec une clé unique et, en guise de protection supplémentaire, crypte la clé elle-même au moyen d'une clé principale qu'il fait régulièrement tourner.

Conformité

En tant que solution de signature électronique conçue pour que les signataires vérifiés puissent interagir avec des documents numériques en tout lieu et sur tous les terminaux, Adobe Sign respecte — ou peut être configuré pour respecter — les exigences de conformité de nombreuses normes du secteur et des organismes de réglementation. Les clients gardent le contrôle de leurs documents, données et workflows, et peuvent choisir la meilleure façon de se conformer aux réglementations locales ou régionales, comme le Règlement général sur la protection des données (RGPD) dans l'UE. Pour de plus amples informations sur la Politique de confidentialité d'Adobe, consultez la page *www.adobe.com/fr/privacy*, et pour en savoir plus sur les lois relatives aux signatures électroniques dans une zone géographique particulière, consultez le *Guide mondial sur la législation en matière de signatures électroniques : synthèse des lois de chaque pays et de leur application*.

ISO 27001
La norme ISO 27001 est publiée par l'ISO (International Organization for Standardization) et l'IEC (International Electrotechnical Commission). Elle contient des exigences pour les systèmes de gestion de la sécurité de l'information (ISMS) qui peuvent être vérifiées par une autorité de certification indépendante et accréditée. Adobe Sign est certifié ISO 27001 : 2013.

SOC
Les contrôles SOC (Service Organization Controls) sont une série de contrôles informatiques pour la sécurité, la disponibilité, l'intégrité du traitement et la confidentialité (Type 2). Adobe Sign est certifié SOC 2 Type 2 (sécurité et disponibilité).

PCI DSS
PCI DSS (Payment Card Industry Data Security Standard) est une norme de sécurité de l'information propriétaire conçue pour aider les entreprises qui gèrent les cartes de crédit des principaux émetteurs à mieux contrôler la gestion des données des porteurs de cartes et réduire la fraude. Adobe Sign, l'un des services proposés dans le cadre d'Adobe Document Cloud, possède une attestation de conformité PCI DSS (commerçants et prestataires de services).

FedRAMP
FedRAMP (Federal Risk and Authorization Management Program) offre une approche normalisée pour l'évaluation de la sécurité, l'autorisation et la surveillance permanente des produits et services cloud utilisés par les agences fédérales américaines. FedRAMP Tailored est la référence pour les prestataires de services cloud avec systèmes SaaS à faible impact (LI-SaaS). Adobe Sign est certifié FedRAMP Tailored.

SAFE-BioPharma
Le standard d'identification et de signature numériques SAFE-BioPharma® a été créé par les organismes de contrôle de l'industrie biopharmaceutique pour offrir au niveau mondial une totale garantie des identités dans le cadre des cybertransactions de divers secteurs : biopharmaceutique, biotechnologique et santé. Adobe Sign est certifié SAFE-BioPharma.

HIPAA[3]
L'HIPAA (Health Insurance Portability and Accountability Act) garantit la protection des informations sensibles des patients en établissant des normes pour les transactions de santé électroniques. Adobe Sign peut être utilisé en conformité avec l'HIPAA par tout établissement considéré comme une entité couverte, selon la définition du ministère américain de la Santé et des Services sociaux (HHS), et ayant signé un contrat d'association commerciale (BAA) avec Adobe.

21 CFR Part 11[3]
Le chapitre 21 du Code des règlements fédéraux indique, dans la partie 11 (21 CFR Part 11), les règlements de la FDA (U.S. Food and Drug Administration) applicables aux enregistrements et signatures électroniques.

GLBA[3]
Le GLBA (Gramm-Leach-Bliley Act) établit les règlements que les établissements financiers doivent appliquer pour garantir la confidentialité des informations personnelles des clients. Adobe Sign est en mesure de se conformer au GLBA.

FERPA[3]

Le FERPA (Family Educational Rights and Privacy Act) est conçu pour préserver la confidentialité des dossiers scolaires et des informations d'annuaire des élèves et étudiants américains. Conformément aux directives du FERPA, Adobe Sign est en mesure de s'engager contractuellement à assumer les fonctions de « responsable de l'établissement » pour gérer les données réglementées des étudiants, et permettre à nos clients du secteur Éducation de se conformer aux exigences du FERPA.

Opérations

Adobe applique des pratiques opérationnelles standard, telles que le suivi des performances, pour gérer l'état du service Adobe Sign.

Suivi des performances

Adobe assure un suivi complet pour contribuer à garantir le bon fonctionnement du service Adobe Sign, notamment en effectuant des contrôles de disponibilité, de volume et de performances. Tous ces contrôles sont basés sur des seuils définis et quantifiables, qui indiquent la nécessité de prendre des mesures préventives. Les seuils et processus de contrôle sont revus régulièrement.

Adobe effectue également une journalisation côté serveur de l'activité des clients pour diagnostiquer les interruptions de service, problèmes spécifiques et autres bogues signalés. Les journaux ne stockent pas d'informations personnelles, comme les mots de passe ou les noms, à l'exception de l'Adobe ID, le cas échéant. L'équipe de support technique, les ingénieurs concernés et certains développeurs sont les seuls à avoir accès aux journaux pour diagnostiquer les problèmes spécifiques susceptibles de se produire.

Gestion du service

Adobe applique les concepts de gestion des services standard, comme la gestion des changements, incidents et problèmes. Nos processus et contrôles sont conçus pour prendre en charge de nombreux cadres de conformité.

Gestion des changements

Adobe applique un processus de gestion des changements standard complet, qui prévoit des inspections rigoureuses pour évaluer les impacts et avantages potentiels des changements apportés au service Adobe Sign. La plupart des changements n'ont aucun impact sur le service. Il existe cependant quelques exceptions, telles que le test annuel des procédures de reprise sur incident, qui peuvent influer sur l'expérience client. Dans ces cas particuliers, Adobe enverra une notification préalable aux clients Adobe Sign susceptibles d'être concernés.

Gestion des incidents

En cas d'interruption de service, l'équipe en charge des opérations Adobe Sign engage le processus de gestion des incidents d'Adobe. Lorsque ce processus est engagé, des ingénieurs d'astreinte 24h/24, 7j/7, 365j/an sont réunis au moyen d'outils de collaboration en ligne afin de diagnostiquer et résoudre le problème. Le processus de gestion des incidents donne également la possibilité de collecter des données sur l'enchaînement des événements ayant conduit à la résolution des incidents, ainsi que des informations permettant d'évaluer l'impact sur nos contrats de niveau de service. Les problèmes en souffrance sont transmis à l'équipe de gestion des problèmes, qui assure la gouvernance continue.

Gestion des problèmes

Dans le cadre du processus de gestion des incidents d'Adobe, une réunion formelle de gestion des problèmes post-mortem est programmée pour examiner la cause première de l'incident et suggérer des actions préventives. Le processus de gestion des problèmes permet aussi de résoudre les incidents détectés lors des pannes, en plus des vulnérabilités ayant contribué à la panne survenue ou risquant fortement d'en provoquer ultérieurement. Le processus de gestion des problèmes comprend une analyse et un résumé de l'incident, une explication détaillée de la cause première, une analyse de l'impact et les mesures correctives requises pour garantir la résolution complète du problème.

[3] Un service Adobe « prêt pour le GLBA », « prêt pour le FERPA » ou conforme à la Réglementation 21 CFR Part 11 de la FDA ou à la loi HIPAA signifie qu'en l'utilisant, le client se conforme aux obligations légales lui incombant au titre du recours à des prestataires de services. Il appartient, en définitive, au client de se conformer à ses obligations légales, c'est-à-dire de veiller à ce que le service Adobe réponde aux impératifs de conformité en le sécurisant convenablement.

Effectifs

Adobe fait appel à une équipe dédiée et géographiquement dispersée d'ingénieurs chargés des opérations techniques, qui travaillent selon le modèle de support inter-régional en continu. Disponible 24h/24, 7j/7, 365j/an, cette équipe internationale aide l'équipe d'Adobe chargée de la résolution des incidents à résoudre les interruptions de service le plus rapidement possible. La plupart des ingénieurs Adobe chargés des opérations techniques sont basés aux États-Unis et à Noida, en Inde.

Gouvernance

Qu'il s'agisse de rechercher les nouvelles vulnérabilités ou de limiter les menaces potentielles, Adobe applique des pratiques standard pour veiller à ce que le processus Adobe Sign de gestion des risques, de limitation des menaces et de résolution des incidents soit à la fois souple et complet.

Gestion des risques

Adobe met un point d'honneur à garantir la souplesse et la précision du processus de gestion des risques et des vulnérabilités, de résolution des incidents et de limitation des menaces. Adobe surveille les menaces en permanence, partage ses informations avec des experts de la sécurité du monde entier et s'efforce de résoudre rapidement les incidents. Tous les fournisseurs d'infrastructure Adobe Sign utilisent plusieurs outils pour détecter, évaluer et suivre proactivement le trafic réseau et d'autres anomalies potentiellement dangereuses, telles que les attaques de déni de service (DoS).

Tests d'intrusion

Adobe approuve et travaille avec des entreprises de sécurité tierces pour réaliser des tests d'intrusion visant à détecter des vulnérabilités potentielles et à améliorer la sécurité globale de ses produits et services. Après réception du rapport établi par le tiers, Adobe documente ces vulnérabilités, évalue les niveaux de gravité et de priorité, et définit une stratégie de limitation des risques ou un plan de réparation pour le service Adobe Sign.

Avant chaque lancement, l'équipe de sécurité d'Adobe Sign soumet le service à une évaluation des risques afin de détecter les éventuelles configurations réseau non sécurisées au niveau des pare-feu, des équilibreurs de charge et du matériel serveur, ainsi que les vulnérabilités au niveau des applications. L'évaluation des risques est réalisée par le personnel de sécurité hautement qualifié chargé de sécuriser la topologie et l'infrastructure du réseau, ainsi que par le service Adobe Sign. Elle prévoit des exercices de modélisation des menaces, ainsi qu'un balayage des vulnérabilités et une analyse statique/dynamique de l'application.

Limitation des menaces

Pour limiter les nouvelles vulnérabilités et menaces qui surgissent quotidiennement, Adobe s'abonne aux listes d'annonces des vulnérabilités du secteur, telles que US-CERT, Bugtraq et SANS, ainsi qu'aux listes d'alertes de sécurité publiées par les principaux éditeurs de logiciels de sécurité. Pour les services cloud comme Adobe Sign, Adobe centralise les décisions relatives aux incidents et à leur résolution, ainsi que le suivi externe, ce qui garantit une cohérence transversale et une résolution rapide des problèmes.

En cas d'annonce d'une faille majeure constituant un risque pour Adobe Sign, les équipes compétentes au sein du pôle Adobe Document Cloud sont informées et peuvent ainsi coordonner les efforts de sécurité. De plus, en cas d'incident, les équipes de résolution et de développement appliquent les pratiques standard suivantes pour identifier, limiter et éliminer les risques :

- Évaluation de l'état de la vulnérabilité
- Limitation des risques liés aux services de production
- Mise en quarantaine, étude et destruction des nœuds compromis (services cloud uniquement)
- Mise au point d'un correctif pour la vulnérabilité
- Déploiement du correctif afin de contenir le problème
- Surveillance de l'activité et confirmation de la résolution des incidents

Pour faciliter l'analyse d'un incident, l'équipe Adobe Sign capture une image complète (ou procède au vidage de la mémoire) de la/des machine(s) concernée(s), conserve les preuves et enregistre la chaîne de traçabilité.

Reprise sur incident

Les centres de données Adobe Sign offrent une résilience élevée, et sont conçus pour garantir un haut niveau de disponibilité et de tolérance aux pannes système ou matérielles, avec un minimum d'impact. Afin de garantir la continuité des opérations, Adobe a recours à des plans régionaux de reprise sur incident pour Adobe Sign lorsque cette solution est hébergée sur l'infrastructure AWS aux États-Unis et au sein de l'UE, ainsi qu'à une documentation sous forme de livre d'exécution annuel décrivant toutes les étapes requises pour le basculement d'un centre de données. Par ailleurs, Adobe s'efforce d'appliquer les paramètres de reprise sur incident suivants pour ses clients Adobe Sign :

- **Objectif de point de reprise (RPO)** — Quantité de données qui pourraient être perdues lors d'une reprise sur incident. Le délai dépend du temps écoulé entre les événements de protection des données. L'objectif RPO d'Adobe Sign est de 2 heures.
- **Objectif de temps de reprise (RTO)** — Temps d'immobilisation potentiel. Cet indicateur correspond au temps nécessaire à la reprise et au rétablissement du service après une perte de données. L'objectif RTO d'Adobe Sign est de 8 heures.

Notification des clients

Les données sur la disponibilité d'Adobe Sign sont accessibles à l'adresse suivante : *www.adobe.com/go/trust-dc-fr*. En outre, pour les temps d'immobilisation système planifiés et non planifiés, Adobe Sign informe les clients de l'état du service par le biais d'un processus de notification.

Si le service opérationnel doit être transféré d'un site principal vers un site de reprise sur incident, les clients reçoivent plusieurs notifications :

- une notification de l'intention de transférer les services vers le site de reprise sur incident ;
- des mises à jour horaires concernant l'avancement de la migration des services ;
- une notification de la fin du transfert vers le site de reprise sur incident.

Ces notifications incluent également les informations de contact et de disponibilité des représentants du support et du succès client. Ces derniers répondent aux questions et aux préoccupations durant et après la migration afin de permettre une transition fluide vers les nouvelles opérations actives sur un autre site régional.

Isolation/séparation des données

Tous les partenaires de services cloud utilisent de puissantes fonctions de contrôle et d'isolement pour séparer les données clients d'Adobe Sign au sein du service multilocataire. Des processus de gestion et autres contrôles de sécurité sont également utilisés pour garantir un isolement et une protection adéquats des données clients.

Pour plus d'informations

Informations détaillées sur la solution : *www.adobe.com/go/adobesign-fr*

Validité juridique des signatures électroniques :
https://acrobat.adobe.com/fr/fr/sign/capabilities/electronic-signature-legality.html

Sécurité Adobe : *www.adobe.com/fr/security*

Centre de données Adobe : *www.adobe.com/fr/trust.html*

Sécurité Microsoft Azure : *azure.microsoft.com/fr-fr/services/security-center*

Sécurité Amazon Web Services : *https://aws.amazon.com/fr/security*

Aide d'Adobe Sign/Activation de l'authentification unique (SSO) avec SAML :
https://helpx.adobe.com/fr/sign/help/SAML_Configuration.html

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
États-Unis
www.adobe.com, www.adobe.com/fr

6/18