Sécurité d'Adobe Digital Publishing Suite, édition Enterprise

Sommaire

Sécurité Adobe

Adobe attache une grande importance à la sécurité des expériences numériques. Depuis l'intégration de la sécurité dans le processus et les outils de développement logiciel en interne, jusqu'à la résolution des incidents par nos équipes pluridisciplinaires, nous nous efforçons d'être proactifs et réactifs. De plus, notre collaboration avec des partenaires, chercheurs et autres acteurs du secteur nous aide à mieux appréhender les meilleures pratiques actuelles en matière de sécurité, et à en tenir compte dans notre offre de produits et services.

Cet article technique décrit l'approche proactive et les procédures mises en œuvre par Adobe pour renforcer la sécurité de votre expérience Adobe Digital Publishing Suite et des données figurant dans les applications créées avec cette plate-forme.

À propos d'Adobe Digital Publishing Suite, édition Enterprise

Adobe Digital Publishing Suite, édition Enterprise est une plate-forme complète de publication de contenu pour terminaux mobiles, qui permet aux groupes de presse, multinationales et établissements d'enseignement supérieur de créer, publier, commercialiser et évaluer les expériences de lecture numérique sur tablettes et smartphones. Digital Publishing Suite est un ensemble de services hébergés et de technologies de lecture étroitement intégrés aux produits Adobe Creative Cloud — dont InDesign — et à Adobe Experience Manager, pour publier des magazines numériques, renforcer l'affinité avec la marque, favoriser les ventes et développer des applications de communication marketing sur terminaux mobiles.

Tous les services inclus dans Adobe Digital Publishing Suite, édition Enterprise, de même que le le lecteur Adobe Content Viewer for Web, sont hébergés sur le cloud. Les autres composants de lecture, notamment Content Viewer for Desktop, se trouvent sur leur plate-forme ou système respectif.

Principaux composants d'Adobe Digital Publishing Suite, édition Enterprise

Digital Publishing Suite est une plate-forme complète de publication d'applications orientées contenu. Pour créer du contenu destiné à être publié sur une application installée sur un terminal mobile, vous devez disposer du logiciel Adobe InDesign ou avoir accès à Adobe Experience Manager.

Si vous utilisez Adobe InDesign :

Après avoir créé du contenu sur votre poste de travail avec Adobe InDesign, vous le convertissez en fichier .folio qui, outre le contenu lui-même, contient les images, les polices et le manifeste associés. Le fichier .folio est ensuite automatiquement chargé dans Digital Publishing Suite via une connexion HTTP sécurisée (HTTPS). Vous pouvez alors gérer et publier le fichier .folio — ou regrouper plusieurs de ces fichiers — sous la forme d'une application qui sera distribuée aux lecteurs.

Si vous utilisez Adobe Experience Manager :

Après avoir créé le contenu dans un modèle HTML à l'aide de l'interface de type glisser-déposer d'Adobe Experience Manager, vous synchronisez le modèle avec Digital Publishing Suite via une connexion HTTP sécurisée (HTTPS). Vous pouvez ensuite créer et publier le fichier .folio — ou regrouper plusieurs de ces fichiers — sous la forme d'une application qui sera distribuée aux lecteurs.

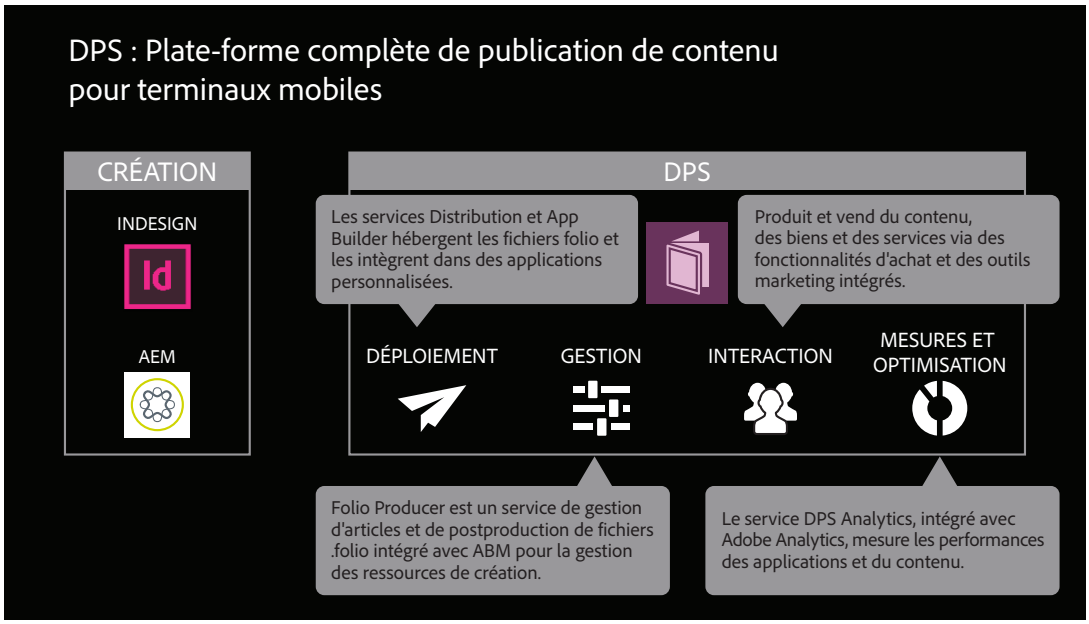
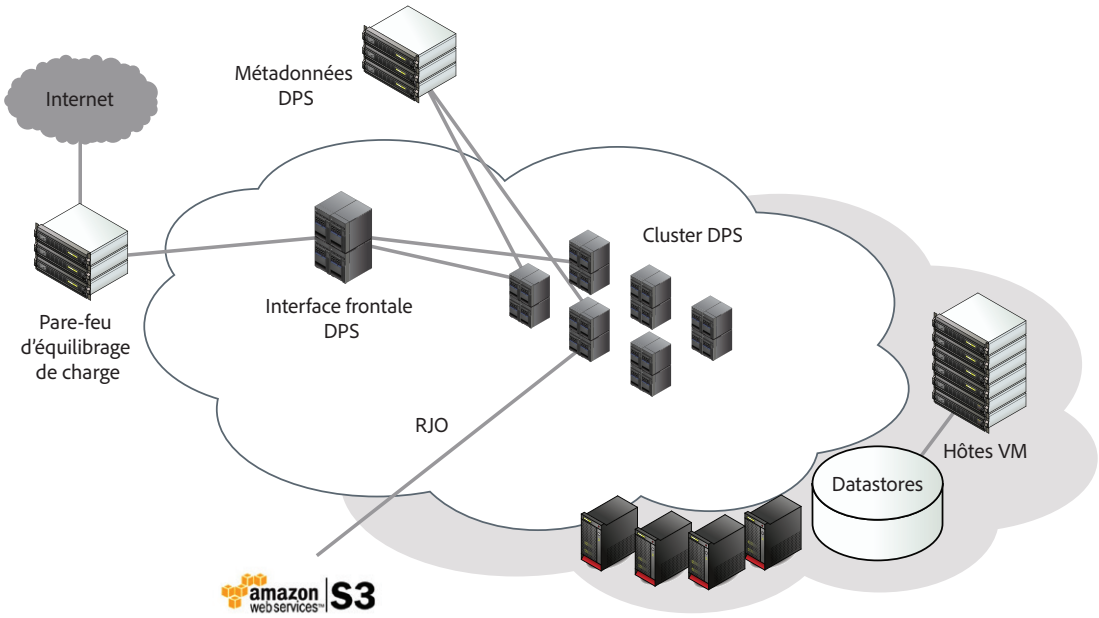


Plate-forme de publication de contenu mobile Adobe Digital Publishing Suite

Adobe Digital Publishing Suite, édition Enterprise inclut les composants suivants :

Service Folio Producer : Permet de partager, gérer et publier des fichiers .folio. Après avoir transféré vos fichiers .folio depuis InDesign ou synchronisé vos modèles HTML depuis Adobe Experience Manager avec le service Folio Producer, vous pouvez assembler et réagencer votre contenu, lui ajouter des métadonnées et prévisualiser le fichier .folio complet tel qu'il s'affichera une fois publié. Le service Folio Producer, qui est hébergé dans le cloud sur AWS (Amazon Web Services), prend en charge de nombreux formats de fichier, dont PDF, JPEG et HTML5.



Topologie réseau du service Folio Producer

DPS App Builder : Permet de télécharger des icônes et ressources permettant de créer une application personnalisée qui sera distribuée via les principales places de marché applicatives ou simplement publiée au sein de votre entreprise. Grâce à cet outil, vous pouvez créer des applications à partir d'un ou de plusieurs fichiers .folio. Vous pouvez également personnaliser la barre d'outils de vos applications en y ajoutant jusqu'à sept icônes différentes.

Service Distribution : Permet le stockage et l'hébergement sécurisés de contenus numériques au format .folio sur les principaux smartphones et tablettes. Lorsque vous activez la fonction de sécurisation du contenu, le service Distribution sécurise également la distribution du contenu numérique. Pour en savoir plus sur la distribution de contenu sécurisé, reportez-vous à la section « Contenu sécurisé et distribution restreinte dans Digital Publishing Suite ».

Service Analytics : Les rapports prédéfinis de ce service permettent de visualiser des indicateurs clés sur les applications, fichiers folio, terminaux, achats et lecteurs, notamment le nombre total d'applications téléchargées et d'autres statistiques sur les achats et l'interaction entre les clients et le contenu. Si vous disposez d'Adobe Analytics, vous avez en outre accès à des rapports plus détaillés que vous pouvez adapter aux besoins de votre activité.

Paramètres d'administration de comptes : Permettent aux administrateurs de gérer les configurations et paramètres de tous les comptes DPS de leur entreprise. Ils peuvent notamment activer la sécurisation du contenu en fonction des rôles. Ils peuvent également activer, désactiver et configurer Adobe Content Viewer for Web à l'aide d'une série de formulaires web et, le cas échéant, fournir les détails nécessaires pour lier le service DPS Analytics à votre compte Adobe Analytics.

Adobe Content Viewer : Offre une expérience de lecture captivante sur Apple iOS et les principaux smartphones et tablettes Android,™ mais aussi sur les postes de travail, tablettes et téléphones équipés de Microsoft® Windows® 8.1. Vous pouvez en outre créer un lecteur de contenu personnalisé pour plonger vos lecteurs et clients dans l'univers graphique de votre publication.

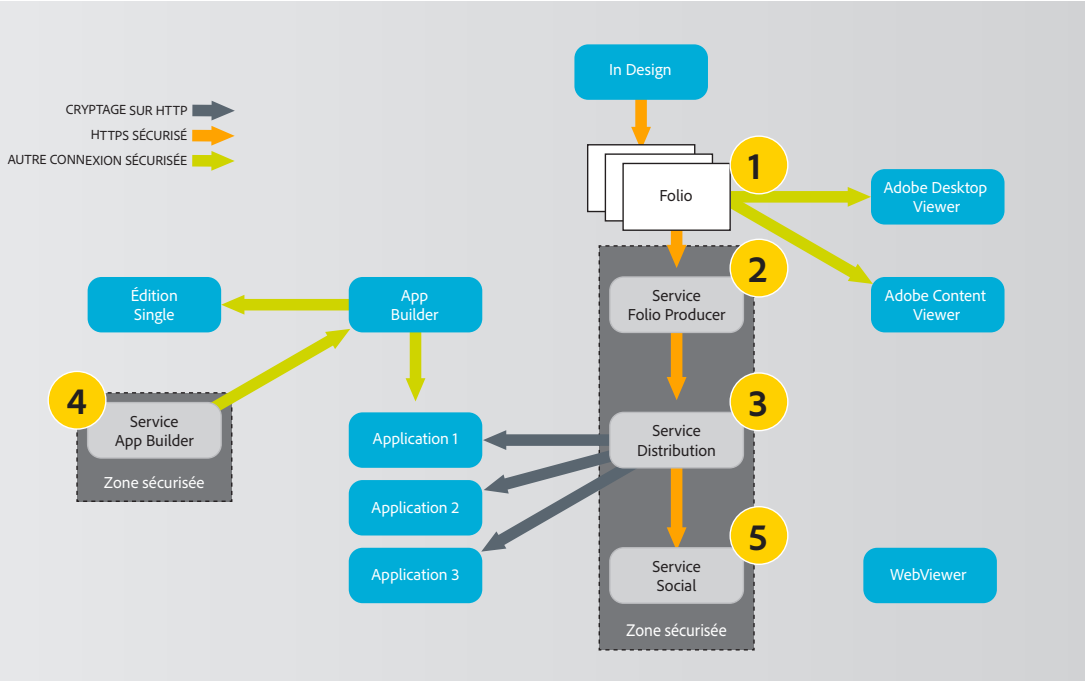
Flux du contenu Adobe Digital Publishing Suite

Pour mieux comprendre Adobe Digital Publishing Suite et les problèmes de sécurité, découvrons à présent le flux du contenu, du développement à la distribution.

Étape 1 : Comme indiqué précédemment, vous utilisez Adobe InDesign ou Adobe Experience Manager pour créer du contenu stocké dans un fichier .folio. Outre le contenu, ce fichier contient les images, les polices et le manifeste associés. Vous pouvez ensuite afficher, actualiser et prévisualiser le contenu sur votre poste de travail à l'aide de **Content Viewer for Desktop**, qui permet d'interagir avec le contenu comme s'il avait été déployé sur une application pour tablette, téléphone ou tout autre terminal mobile.

Si vous utilisez InDesign, le fichier .folio est automatiquement transféré vers le service Folio Producer. Si vous créez du contenu avec Adobe Experience Manager, un simple clic sur le bouton Synchroniser permet de synchroniser votre modèle HTML avec le service Folio Producer pour passer à l'étape suivante.

Remarque : Adobe conseille de ne pas insérer d'informations personnelles ou confidentielles dans les fichiers .folio. Si vous le faites malgré tout, il est préférable d'activer la fonction de sécurisation du contenu. Cependant, cette fonction désactive d'autres fonctionnalités de Digital Publishing Suite. Avant d'activer la fonction de sécurisation du contenu, pesez soigneusement le pour et le contre. Pour plus d'informations, reportez-vous à la section « Contenu sécurisé et distribution restreinte dans Digital Publishing Suite » ci-après.



Flux du contenu Adobe Digital Publishing Suite – Contenu sécurisé

Étape 2 : Votre contenu est automatiquement chargé depuis InDesign dans Adobe Experience Manager, ou synchronisé entre ce dernier et le **service Folio Producer** via une connexion HTTPS sécurisée. Les utilisateurs autorisés peuvent alors visualiser et tester le contenu à l'aide d'**Adobe Content Viewer** — une application mobile d'Adobe — sous iOS, les principaux terminaux mobiles Android et ceux équipés de Windows 8.1.

Étape 3 : Lorsque votre contenu est prêt à être publié, cliquez sur « Publier » dans le service Folio Producer pour l'envoyer au **service Distribution** via une connexion HTTPS sécurisée.

Par défaut, le service Distribution stocke le contenu sous forme non cryptée. Toutefois, si vous activez la fonction de sécurisation du contenu, il sera crypté avant stockage. Lorsqu'un internaute télécharge du contenu, celui-ci est mis en cache sur des serveurs Edge détenus par un réseau de données de contenu (actuellement Akamai) et stocké dans le même format (crypté ou non, par exemple) que dans le service Distribution.

Si vous activez la fonction de sécurisation du contenu, celui-ci est crypté dans le service Distribution et décrypté une fois téléchargé sur le terminal du lecteur, où il est ensuite protégé par les dispositifs de sécurité du système d'exploitation.

Étape 4 : Si vous souhaitez créer une application personnalisée pour héberger votre contenu, vous pouvez utiliser **DPS App Builder.** Les clients peuvent ensuite télécharger le contenu le plus récent depuis leur application.

Étape 5 : Si vous voulez que votre contenu puisse être partagé via les réseaux sociaux — comme Facebook et Twitter — à l'aide d'un navigateur web, vous pouvez utiliser le **service d'administration de comptes**. Une fois cette fonctionnalité activée, les utilisateurs peuvent partager tout ou partie d'un article via un lien. L'accès à ce contenu est également possible sur terminaux mobiles via **Adobe Content Viewer** for Web, dans un format similaire.

** Remarque : si vous avez activé la fonction de sécurisation du contenu, le partage sur les réseaux sociaux est automatiquement désactivé. Pour plus d'informations, reportez-vous à la section « Contenu sécurisé et distribution restreinte dans Digital Publishing Suite » ci-après.*

Étape 6 : Pendant la durée de validité de votre contrat, vous pouvez à tout moment supprimer un fichier .folio publié. Si vous résiliez votre abonnement Digital Publishing Suite, le contenu publié restera sur les serveurs Digital Publishing Suite pendant au moins 90 jours après la date de résiliation. Passé ce délai, Adobe se réserve le droit de supprimer le contenu de ses serveurs selon ses besoins.

Contenu sécurisé et distribution restreinte dans Digital Publishing Suite

Si vos fichiers .folio contiennent des informations personnelles ou si vous souhaitez autoriser certains utilisateurs à accéder à un contenu spécifique, vous pouvez utiliser la fonction de sécurisation du contenu de Digital Publishing Suite. Cette fonction n'est disponible que dans Digital Publishing Suite version 30 ou ultérieure pour les applications soumises à des droits directs et au détail, et prend uniquement en charge les applications Apple iOS disponibles à ce jour.

Elle permet de limiter la distribution du contenu en fonction de l'identité ou du rôle de l'utilisateur. Par exemple, si vous représentez un laboratoire pharmaceutique, vous pouvez accorder l'accès à certains contenus aux médecins, tandis que les commerciaux n'auront accès qu'à une partie de ces données ou à un tout autre contenu.

Pour activer la sécurisation du contenu, vous devez configurer votre propre serveur de droits, qui détermine le contenu visible et les utilisateurs autorisés, plutôt que de faire appel à une boutique d'applications pour distribuer les vôtres. Pour plus d'informations sur les droits directs, reportez-vous à la page *www.adobe.com/devnet/digitalpublishingsuite/entitlement.html*

Le workflow de création et de distribution d'applications sécurisées se déroule en trois étapes :

1. Avant de commencer, activez la protection des données dans l'iOS Developer Center. Cette opération active le mode sécurisé de votre terminal mobile et place votre contenu sous la protection des fonctions de sécurité du système d'exploitation.
2. Dans l'outil Administration de comptes de Digital Publishing Suite, cochez la case « Activer le contenu sécurisé » ; cela autorise le compte de l'éditeur de contenu — lié à son identifiant Adobe — à créer du contenu sécurisé.
3. Lorsque votre contenu sécurisé est prêt à être publié dans le service Folio Producer, sélectionnez l'option « Chiffrer le Folio », désignez le fichier .folio comme « Public » et attribuez-lui le statut « Commercialisé ».

Mécanismes de sécurité activés et contenu sécurisé

Lorsque vous créez du contenu sécurisé, les mécanismes de sécurité supplémentaires suivants s'appliquent :

- Lorsque vous chargez les fichiers .folio dans le service Folio Producer, ils sont stockés dans un conteneur (« bucket ») AWS S3 (Amazon Simple Storage Service) sécurisé. Cela signifie également que vous ne pouvez pas utiliser Adobe Content Viewer for Web pour tester ou prévisualiser le contenu tant qu'il réside dans le service Folio Producer.
- Pour tester ou prévisualiser du contenu sécurisé, vous devez le publier dans le service Distribution. Pour ce faire, sélectionnez l'option « Chiffrer le Folio », désignez le fichier .folio comme « Public » et attribuez-lui le statut « Commercialisé » dans le service Folio Producer. Le fichier .folio et son contenu sont ensuite publiés sous forme cryptée dans le service Distribution. À ce stade, vous pouvez le tester et le prévisualiser via l'option « Afficher l'aperçu sur le périphérique », qui utilise Adobe Content Viewer sur le terminal mobile de destination.
- Tous les fichiers .folio utilisant la fonction de sécurisation du contenu et l'option « Chiffrer le Folio » sont cryptés lors de leur diffusion sur l'application mobile. Ils restent cryptés lorsque le terminal est verrouillé ou hors tension. Une fois l'appareil déverrouillé par mot de passe ou Touch ID, le contenu des fichiers .folio est décrypté et devient disponible. Ce mécanisme utilise la fonctionnalité Apple iOS standard du système d'exploitation. Pour plus d'informations sur les applications sécurisées, consultez le *document sur la sécurité d'Apple iOS*.

Restrictions et limitations du contenu sécurisé

La fonction de sécurisation du contenu permet de restreindre la distribution de contenu confidentiel ou sensible en fonction de l'identité ou du rôle de l'utilisateur, et limite également d'autres fonctions de Digital Publishing Suite. Ces restrictions sont les suivantes :

- Le cryptage est disponible uniquement pour les fichiers .folio publics de statut « Commercialisé ».
- Le partage du contenu sur les réseaux sociaux est désactivé.
- La prévisualisation sans fil des fichiers .folio sécurisés via le service Folio Producer avec Adobe Content Viewer for Web est désactivée pour des raisons de sécurité. Pour prévisualiser des fichiers .folio sécurisés stockés dans le service Distribution, utilisez l'option « Afficher l'aperçu sur le périphérique ».
- Le téléchargement en arrière-plan et le téléchargement progressif ne sont pas pris en charge. Le fichier .folio doit être entièrement téléchargé sur le terminal avant d'être décrypté.

Stockage et options de stockage de Digital Publishing Suite

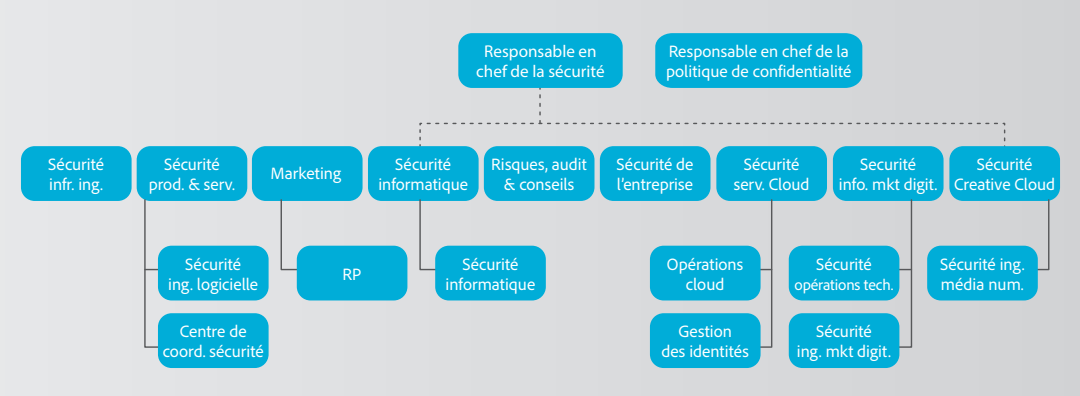
Le contenu chargé dans le service Folio Producer est stocké dans le cloud sur Amazon S3, une infrastructure qui permet de stocker et d'extraire des données, quel que soit leur volume. Les clients d'Adobe Digital Publishing Suite gardent constamment la maîtrise de leurs données, dont ils restent propriétaires. Pour en savoir plus, lisez les *Conditions d'utilisation* et la *Politique de confidentialité* d'Adobe.

Le service Folio Producer lie la totalité du contenu stocké à un identifiant Adobe spécifique, dont il se sert pour séparer ce contenu de manière virtuelle. Même si le service Folio Producer ne crypte pas le contenu archivé, il le stocke dans un format inaccessible aux services Adobe autres que les services Folio Producer et Distribution, l'API du service Folio Producer ou le panneau Folio Builder d'InDesign (Acrobat.com, par exemple).

Pôle de sécurité Adobe

Tous les efforts de sécurité déployés par Adobe sont placés sous l'autorité du responsable en chef de la sécurité (CSO). Le bureau du CSO coordonne l'ensemble des initiatives de sécurité concernant les produits et services ainsi que la mise en œuvre du processus *Adobe SPLC (Secure Product Lifecycle)*.

Le CSO dirige également l'ASSET (Adobe Secure Software Engineering Team), une équipe centrale dédiée, composée de spécialistes de la sécurité qui dispensent des conseils aux équipes en charge des opérations et produits Adobe, dont Adobe Digital Publishing Suite. Les chercheurs ASSET collaborent avec chacune de ces équipes pour assurer un niveau de sécurité adapté aux différents produits et services et les conseillent sur les pratiques de sécurité qui leur permettront de mettre en place des processus clairs et reproductibles en matière de développement, de déploiement, d'opérations et de résolution des incidents.



Pôle de sécurité Adobe

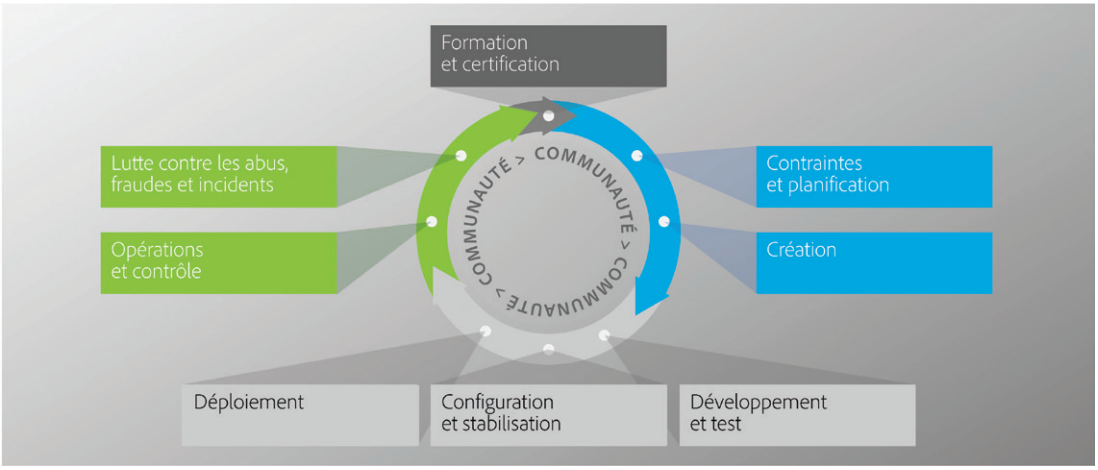
Développement sécurisé des produits Adobe

À l'instar des autres grands pôles dédiés aux produits et services Adobe, le pôle Digital Publishing applique le processus SPLC. Regroupant plusieurs centaines d'activités de sécurité liées aux pratiques, processus et outils de développement logiciel, Adobe SPLC est intégré à plusieurs étapes du cycle de vie du produit, de la création au déploiement, en passant par le développement, les tests et l'assurance qualité. Les chercheurs ASSET fournissent des conseils sur l'utilisation du processus SPLC pour chaque produit et service en se basant sur une évaluation des risques potentiels de sécurité. Bénéficiant en outre du soutien permanent de la communauté, Adobe SPLC évolue au rythme des dernières tendances en matière de technologies, de pratiques de sécurité et de menaces.

Processus Adobe SPLC

Les activités Adobe SPLC varient en fonction du composant Digital Publishing Suite. Elles peuvent inclure tout ou partie des meilleures pratiques, processus et outils suivants :

- Formation et certification de sécurité pour les équipes produit
- Analyse de l'intégrité, des risques et des menaces associés aux produits
- Modalités, règles et analyses de programmation sécurisées
- Feuilles de route des services, outils de sécurité et méthodes de test pour aider l'équipe en charge de la sécurité d'Adobe Digital Publishing Suite à résoudre les dix principales failles des applications web recensées par l'OWASP (Open Web Application Security Project) et les 25 erreurs de programmation les plus dangereuses répertoriées dans le rapport CWE/SANS.
- Étude de l'architecture de sécurité et tests d'intrusion
- Analyses du code source pour favoriser l'élimination des failles connues pouvant provoquer des vulnérabilités
- Validation du contenu créé par les utilisateurs
- Analyse du code statique et dynamique
- Analyse des applications et du réseau
- Analyse d'aptitude, plans de réponse et publication de supports de formation pour les développeurs



Processus Adobe SPLC

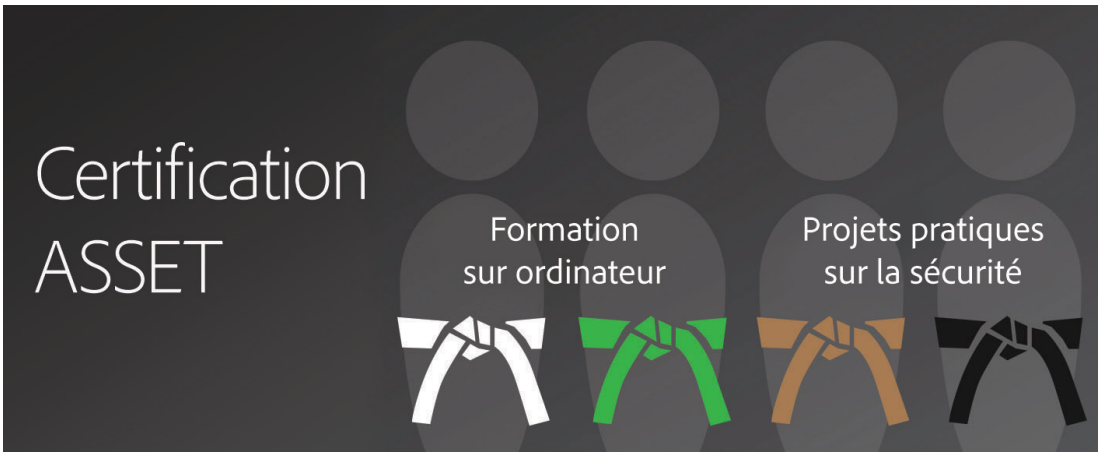
Formation Adobe sur la sécurité

Programme de certification ASSET

Dans le cadre du processus SPLC, Adobe dispense des formations continues aux équipes de développement afin de mieux les sensibiliser aux questions de sécurité et de renforcer la sécurité globale des produits et services. Les employés participant à ce programme de certification atteignent différents niveaux de certification en réalisant des projets de sécurité.

Le programme comporte quatre niveaux, chacun d'entre eux étant symbolisé par une couleur : blanc, vert, marron et noir. Les niveaux blanc et vert sont atteints suite à une formation sur ordinateur. Les niveaux supérieurs, marron et noir, nécessitent une participation de plusieurs mois ou d'une année complète à des projets de sécurité. Les collaborateurs qui atteignent ces deux niveaux deviennent des experts de la sécurité au sein de leur équipe produit. Les formations Adobe sont régulièrement actualisées afin de couvrir les nouvelles menaces et options de limitation des risques, ainsi que les nouveaux langages logiciels.

Plusieurs équipes du pôle Digital Publishing Suite participent également à des ateliers et formations de sensibilisation afin de mieux comprendre en quoi la sécurité influe sur leurs rôles au sein du pôle en lui-même et de l'entreprise toute entière.



Programme de certification ASSET

Hébergement d'Adobe Digital Publishing Suite

Tous les composants d'Adobe Digital Publishing Suite sont hébergés sur AWS, et notamment Amazon Elastic Compute Cloud (Amazon EC2) et Amazon Simple Storage Service (Amazon S3), aux États-Unis, en Europe et en Asie-Pacifique. Amazon EC2 est un service web fournissant des fonctions de calcul modulables sur le cloud. Amazon S3 est une infrastructure hautement redondante qui permet de stocker et d'extraire des données, quel que soit leur volume, à tout moment et en tout lieu.

La plate-forme AWS propose des services conformes aux pratiques standard et passe régulièrement les certifications et audits reconnus sur le marché. Pour en savoir plus sur AWS et les contrôles de sécurité d'Amazon, consultez la *page du site web d'Amazon dédiée à la sécurité*.

Responsabilités d'AWS et d'Adobe

AWS exploite, gère et contrôle les composants Digital Publishing Suite depuis la couche de virtualisation (l'hyperviseur) jusqu'à la sécurité physique des sites où ils sont hébergés. Adobe est, pour sa part, responsable de la gestion du système d'exploitation invité (y compris les mises à niveau et correctifs de sécurité) et des logiciels applicatifs, ainsi que de la configuration du pare-feu du groupe de sécurité fourni par AWS.

AWS gère également l'infrastructure cloud qu'utilise Adobe pour allouer des ressources informatiques élémentaires, notamment pour le traitement et le stockage des données. L'infrastructure AWS comprend des sites, des réseaux, des équipements, mais aussi des logiciels (systèmes d'exploitation hôtes, logiciels de virtualisation, etc.) prenant en charge l'allocation et l'utilisation de ces ressources. Amazon a conçu et gère AWS conformément aux pratiques standard et à de nombreuses normes de sécurité.

Gestion sécurisée

Adobe utilise les protocoles SSH (Secure Shell) et SSL (Secure Sockets Layer) pour gérer les connexions à l'infrastructure AWS.

À propos des services AWS (Amazon Web Services)

Emplacement géographique des données clients sur le réseau AWS

Les informations qui suivent sont tirées de l'article technique AWS : Overview of Security Processes (AWS : Présentation des processus de sécurité). Pour plus de détails sur la sécurité d'AWS, consultez l'*article technique AWS*.

Adobe stocke toutes les données clients Digital Publishing Suite dans la région Est d'AWS aux États-Unis. Pour les clients résidant aux États-Unis, Adobe stocke les données analytiques sur les sites AWS de San Jose (Californie) et Dallas (Texas). Pour les clients hors des États-Unis, ces données sont stockées sur le site AWS de Londres (Royaume-Uni).

Les objets de données Amazon S3 sont uniquement répliqués au sein du cluster régional où les données sont stockées.

Isolement des données clients/séparation des clients

AWS utilise de puissantes fonctions de contrôle et d'isolement. En tant qu'environnement virtualisé multilocataire, AWS met en œuvre des processus de gestion de la sécurité et applique divers contrôles en vue d'isoler chaque client, notamment les clients Digital Publishing Suite, des clients AWS. Adobe utilise en outre le système IAM (Identity and Access Management) d'AWS pour restreindre l'accès aux instances de calcul et de stockage.

Architecture réseau sécurisée

AWS utilise des équipements réseau, notamment des pare-feu et autres systèmes de protection pour contrôler les communications qui transitent à l'intérieur et à l'extérieur du réseau. Ces équipements 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 administrée pour assurer et gérer le trafic. L'équipe Amazon Information Security valide l'ensemble des règles ACL et les transfère automatiquement vers chaque interface administrée à l'aide de l'outil ACL-Manage d'AWS. Les listes ACL sont ainsi parfaitement à jour.

Contrôle et protection du réseau

AWS utilise 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 de communication (entrées et sorties).

Le réseau AWS offre une solide protection contre les problèmes de sécurité réseau classiques :

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

Pour en savoir plus sur le contrôle et la protection du réseau, consultez l'article technique *AWS: Overview of Security Processes (AWS : Présentation des processus de sécurité)* sur le site web d'Amazon.

Détection des intrusions

Adobe supervise activement les services Folio Producer et Distribution au moyen de systèmes de détection et de prévention des intrusions standard.

Consignation

Adobe effectue une journalisation côté serveur de l'activité des clients Digital Publishing Suite pour diagnostiquer les interruptions de service, problèmes spécifiques des clients et autres bogues signalés. Pour faciliter l'analyse de ces incidents, les journaux stockent uniquement les identifiants Adobe et ne contiennent aucune combinaison nom d'utilisateur/mot de passe. 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.

Contrôle de la qualité du service

AWS contrôle les systèmes et équipements électriques, mécaniques et de survie afin de repérer immédiatement les éventuels problèmes techniques. Une maintenance préventive est assurée en continu pour garantir le bon fonctionnement de ces équipements.

Stockage et sauvegarde des données

Adobe stocke la totalité des données Digital Publishing Suite sur Amazon S3, une infrastructure de stockage à haute durabilité. Pour préserver cette durabilité, les fonctions PUT et COPY d'Amazon S3 stockent en mode synchrone les données des clients sur plusieurs sites. Les objets sont, quant à eux, stockés de façon redondante sur plusieurs équipements dans divers centres d'une même région Amazon S3. Par ailleurs, Amazon S3 détecte les corruptions de paquets de données lors des opérations de stockage et d'extraction par le biais de sommes de contrôle. Pour plus de détails sur la sécurité d'AWS, consultez l'article technique *AWS: Overview of Security Processes (AWS : Présentation des processus de sécurité)*.

Gestion des changements

Les changements routiniers, en urgence et de configuration apportés à l'infrastructure AWS existante sont autorisés, consignés, testés, validés et documentés conformément aux normes sectorielles des systèmes similaires. Les mises à jour d'AWS sont programmées par Amazon de façon à limiter l'impact côté clients. Ces derniers sont informés par e-mail ou via l'*AWS Service Health Dashboard* des perturbations potentielles du service. Adobe gère également un *tableau de bord sur l'état* d'Adobe Digital Publishing Suite.

Gestion des correctifs

AWS est responsable des systèmes de correction permettant d'accéder à ses services, comme l'hyperviseur et les services de mise en réseau. Adobe prend en charge l'application de correctifs pour ses systèmes d'exploitation (OS) invités, logiciels et applications exécutés dans AWS. Lorsque des correctifs sont nécessaires, Adobe propose une nouvelle instance à sécurité renforcée du système d'exploitation et de l'application plutôt qu'un correctif à proprement parler.

Authentification des utilisateurs d'Adobe Digital Publishing Suite (identifiant Adobe)

Après avoir été invités par l'administrateur à rejoindre l'équipe, les utilisateurs doivent créer un identifiant Adobe qui leur permettra d'accéder à Digital Publishing Suite. Cet identifiant associe l'algorithme de hachage SHA 256 à un salage des mots de passe et à un grand nombre d'itérations de hachage. Adobe surveille en permanence les comptes de ses utilisateurs pour identifier les activités inhabituelles ou anormales, et évalue ces informations pour limiter rapidement les menaces.

Stockage des certificats et des clés

DPS App Builder invite les utilisateurs à fournir leur certificat numérique et leur profil afin de signer leurs applications. Les certificats sont stockés en local sur l'ordinateur de signature et ne sont pas transférés à Adobe (ou AWS) pendant le processus.

Pour procéder à la vérification des abonnements, nous demandons aux clients d'enregistrer la clé partagée de leur boutique d'applications pour chaque application créée et disponible sur abonnement. Il s'agit d'une clé privée et Adobe observe les directives d'Apple concernant le transport, le stockage et l'utilisation de cette clé dans le cadre de la vérification des abonnements via le kit SDK iOS.

Les utilisateurs qui choisissent d'utiliser le service de notification push pour iOS d'Adobe doivent charger leur certificat push sur un serveur Adobe. Adobe applique les consignes d'Apple relatives à la gestion des certificats push tiers.

Gestion des risques et vulnérabilités par Adobe

Tests de sécurité

Adobe collabore avec des agences de sécurité agréées pour réaliser des tests d'intrusion en vue de détecter des vulnérabilités potentielles et d'améliorer la sécurité globale de ses produits et services. Après réception du rapport établi par le fournisseur, Adobe documente les vulnérabilités détectées, évalue les niveaux de gravité et de priorité, et définit une stratégie de limitation des risques ou un plan de réparation.

Adobe analyse la sécurité des services Digital Publishing Suite avant le lancement de chaque nouvelle version. Réalisée par des opérateurs hautement qualifiés, chargés de créer une infrastructure et une topologie réseau sécurisées — non seulement pour Digital Publishing Suite mais aussi pour l'ensemble des produits et services Adobe hébergés — , cette analyse vise à identifier les problèmes de configuration réseau non sécurisée sur l'ensemble des pare-feu, dispositifs d'équilibrage de charge et serveurs. Des copies de cette analyse de sécurité préliminaire, soumises à un accord de confidentialité, sont disponibles sur demande.

Les clients peuvent réaliser leur propre analyse de sécurité de l'infrastructure externe pour Digital Publishing Suite en prenant contact avec le *support technique Adobe*. En revanche, ils NE sont PAS autorisés à effectuer des tests d'intrusion ou de charge sur les systèmes Digital Publishing Suite externes. Les contrevenants enfreignent les conditions d'utilisation de Digital Publishing Suite et Adobe se réserve le droit de résilier leur abonnement ou d'interrompre le service.

Résolution et notification des incidents

Adobe met tout en œuvre pour résoudre et limiter les nouvelles vulnérabilités et menaces. La société est d'ailleurs abonnée aux listes d'annonce des vulnérabilités du secteur, notamment US-CERT, Bugtraq et SANS, ainsi qu'aux listes des dernières alertes publiées par les principaux éditeurs de logiciels de sécurité.

Lorsqu'une vulnérabilité est identifiée, l'équipe Adobe PSIRT (Product Security Incident Response Team) communique l'information aux personnes compétentes au sein du pôle Digital Publishing Suite afin de coordonner les efforts de sécurité.

L'équipe Amazon Incident Management utilise pour sa part des procédures de diagnostic standard pour faire face aux incidents, vulnérabilités et menaces susceptibles de nuire à l'activité du centre de données AWS. Des opérateurs se relaient 24 heures sur 24, 7 jours sur 7 et 365 jours par an pour détecter les incidents, gérer leur impact et leur résolution, mais aussi informer Adobe et les autres clients AWS.

Pour Digital Publishing Suite, nous centralisons également les décisions relatives aux incidents et à leur résolution, ainsi que le suivi externe au sein de notre Centre de coordination de la sécurité (SCC), ce qui garantit une cohérence transversale et une résolution rapide des problèmes.

En cas d'incident, l'équipe SCC travaille avec les équipes de développement et de résolution des incidents de Digital Publishing Suite pour identifier, limiter et résoudre le problème en appliquant le processus éprouvé suivant :

- Évaluation de l'état de la vulnérabilité
- Atténuation 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 validation de la résolution des incidents

Analyse scientifique

Dans le cadre de ses investigations sur les incidents, Adobe emploie des outils et méthodologies standard et applique un processus d'analyse scientifique, avec capture d'images complète ou vidage de la mémoire des machines concernées, conservation sécurisée des preuves et enregistrement de la chaîne de traçabilité. Dans certains cas, Adobe peut être amené à faire appel aux services de police ou à des experts scientifiques.

Contrôles physiques et environnementaux des centres de données AWS

Les contrôles physiques et environnementaux AWS sont décrits dans un rapport SOC 1 de type 2. La section ci-dessous présente une partie des mesures et contrôles de sécurité mis en place dans les centres de données AWS du monde entier. Pour plus de détails sur la sécurité d'AWS, consultez l'article technique *AWS : Overview of Security Processes (AWS : Présentation des processus de sécurité)* ou la *page du site web d'Amazon dédiée à la sécurité*.

Sécurité des installations physiques

Les centres de données AWS reposent sur des techniques standard en matière d'architecture et d'ingénierie. Ils sont hébergés sur des sites banalisés. L'accès physique est contrôlé à la fois dans l'enceinte et aux points d'accès du bâtiment par des professionnels de la sécurité, des systèmes de vidéo-surveillance et de détection d'intrusion, et d'autres moyens électroniques. Le personnel autorisé doit procéder à au moins deux reprises à une authentification à deux facteurs pour pouvoir accéder aux étages des centres de données. Tous les visiteurs et sous-traitants sont tenus de présenter une pièce d'identité. Ils sont enregistrés à leur arrivée, puis accompagnés en permanence de personnes habilitées.

AWS n'autorise l'accès aux centres de données et la diffusion d'informations qu'aux personnes qui en ont besoin à des fins professionnelles. Lorsqu'un employé n'a plus besoin de tels privilèges, son accès est immédiatement révoqué, même s'il fait toujours partie d'Amazon ou d'Amazon Web Services. L'accès physique aux centres de données par le personnel d'AWS est systématiquement consigné et audité.

Extinction d'incendie

Un équipement de détection et d'extinction automatique des incendies est installé dans chaque centre de données AWS. Des détecteurs de fumée sont présents dans tous les centres de données, les sites abritant l'infrastructure mécanique et électrique, les salles de refroidissement et les pièces contenant les générateurs. Ces zones sont protégées soit par des installations d'extinction automatique à eau et à préaction à double verrouillage, soit par des extincteurs automatiques à gaz.

Environnement contrôlé

AWS utilise un système de climatisation pour maintenir une température de fonctionnement constante pour les serveurs et autres équipements, ce qui empêche les surchauffes et réduit les risques d'interruption de service. Les centres de données AWS garantissent le maintien de conditions atmosphériques optimales. La température et l'humidité sont surveillées et régulées par le personnel AWS et différents systèmes.

Alimentation de secours
Les systèmes d'alimentation électrique des centres de données AWS offrent une totale redondance et fonctionnent 24 heures sur 24, 7 jours sur 7, y compris lors des opérations de maintenance. Des systèmes d'alimentation sans interruption (UPS) fournissent une alimentation de secours en cas de panne électrique au niveau des charges critiques et essentielles des installations. Les centres de données utilisent des générateurs pour alimenter l'ensemble des installations en cas de panne.

Vidéo-surveillance
L'accès physique aux centres de données AWS est strictement contrôlé à la fois dans l'enceinte et aux points d'accès du bâtiment par des professionnels de la sécurité, des systèmes de vidéo-surveillance et de détection d'intrusion, et d'autres moyens électroniques.

Reprise sur incident
Les centres de données AWS offrent un haut niveau de disponibilité et de tolérance aux pannes système ou matérielles. Clusterisés dans différentes zones géographiques, ils restent en ligne 24 heures sur 24, 7 jours sur 7 et 365 jours par an. Aucun d'entre eux n'est « inactif ». En cas de panne, le trafic des données clients est automatiquement détourné de la zone impactée. Les applications stratégiques étant déployées selon une configuration N+1, en cas de panne, la capacité reste suffisante pour permettre un équilibrage de charge du trafic vers les autres sites. Pour en savoir plus sur les protocoles de reprise sur incident d'AWS, consultez le *site web d'Amazon*.

Bureaux Adobe
Adobe possède des bureaux dans le monde entier et met en œuvre les procédures et processus suivants pour contrer les menaces de sécurité :

Sécurité physique
Chaque bureau Adobe emploie des gardiens sur site pour protéger les installations 24 heures sur 24, 7 jours sur 7. Les employés disposent d'un badge à leur nom pour accéder au bâtiment. Les visiteurs empruntent l'entrée principale, signent un registre à l'entrée et à la sortie, portent un badge Visiteur temporaire et sont toujours accompagnés d'un employé. Les équipements serveur, machines de développement, systèmes téléphoniques, serveurs de fichiers et de messagerie et autres systèmes sensibles sont systématiquement enfermés dans des salles serveur à environnement contrôlé et uniquement accessibles par le personnel qualifié et autorisé.

Protection contre les virus
Avant de stocker le contenu soumis au service Folio Producer sur ses systèmes, Adobe l'analyse à la recherche d'éventuels virus.

Employés Adobe

Accès des employés aux données clients
Pour Digital Publishing Suite, Adobe segmente les environnements de développement et de production, et applique des contrôles techniques pour limiter l'accès aux systèmes de production en direct à partir du réseau et des applications. Les employés disposent d'autorisations spécifiques pour accéder aux systèmes de développement et de production.

Vérification des antécédents
Adobe obtient des rapports de vérification des antécédents pour ses futurs employés. La société s'intéresse tout particulièrement à leurs parcours universitaire et professionnel, à leur casier judiciaire (y compris les condamnations pénales) et aux références fournies par leurs contacts professionnels et personnels, conformément à la loi en vigueur. Aux États-Unis, ces vérifications d'antécédents concernent les nouvelles recrues, notamment les personnes qui seront chargées d'administrer les systèmes ou qui auront accès aux données des clients. Les nouveaux employés intérimaires sont soumis à ces vérifications par le biais de l'agence de travail temporaire contactée, conformément aux directives d'Adobe. En dehors des États-Unis, Adobe vérifie les antécédents de certaines nouvelles recrues, conformément à sa stratégie de vérification d'antécédents et aux législations locales en vigueur.

Départ des employés

En cas de démission d'un employé Adobe, son responsable soumet un formulaire de sortie. Une fois ce dernier approuvé, le service des ressources humaines d'Adobe adresse un courrier électronique aux personnes compétentes pour les informer des mesures à prendre avant le dernier jour de travail de l'employé. En cas de licenciement d'un employé, le service des ressources humaines d'Adobe envoie un courrier similaire aux personnes compétentes, leur indiquant la date et l'heure de fin du contrat de travail.

Le service de sécurité d'Adobe programme alors les actions suivantes, de sorte que l'employé ne puisse plus avoir accès aux fichiers confidentiels ni aux bureaux d'Adobe une fois son contrat terminé :

- Suppression de l'accès à la messagerie électronique
- Suppression de l'accès VPN à distance
- Désactivation du badge d'accès aux bureaux et aux centres de données
- Suppression de l'accès réseau

Les responsables peuvent éventuellement demander au personnel de sécurité du bâtiment de raccompagner l'employé jusqu'à la sortie des bureaux ou du bâtiment Adobe.

Confidentialité des données clients

Adobe traite les données des clients comme des données confidentielles. Les informations collectées pour le compte d'un client ne sont jamais utilisées ni divulguées, sauf disposition contraire figurant dans le contrat conclu avec ce client et prévue par les *Conditions générales d'utilisation* et la *Politique de confidentialité d'Adobe*.

Principes de la sphère de sécurité (Safe Harbor)

Adobe Systems Incorporated (notre entité américaine) adhère au *programme de confidentialité Safe Harbor de l'Union européenne*.

Respect des normes de sécurité

AWS gère ses propres assertions et initiatives de mise en conformité avec ISO27001, SOC2 et d'autres certifications applicables à la sécurité.

Conclusion

L'approche proactive d'Adobe en matière de sécurité et les procédures rigoureuses décrites dans ce document contribuent à préserver la sécurité de vos données Digital Publishing Suite. Adobe attache une grande importance à la sécurité des expériences numériques.

Pour en savoir plus sur les mesures de sécurité appliquées à l'ensemble de nos produits et services, consultez le *site d'information sur la sécurité* d'Adobe.

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

5/14