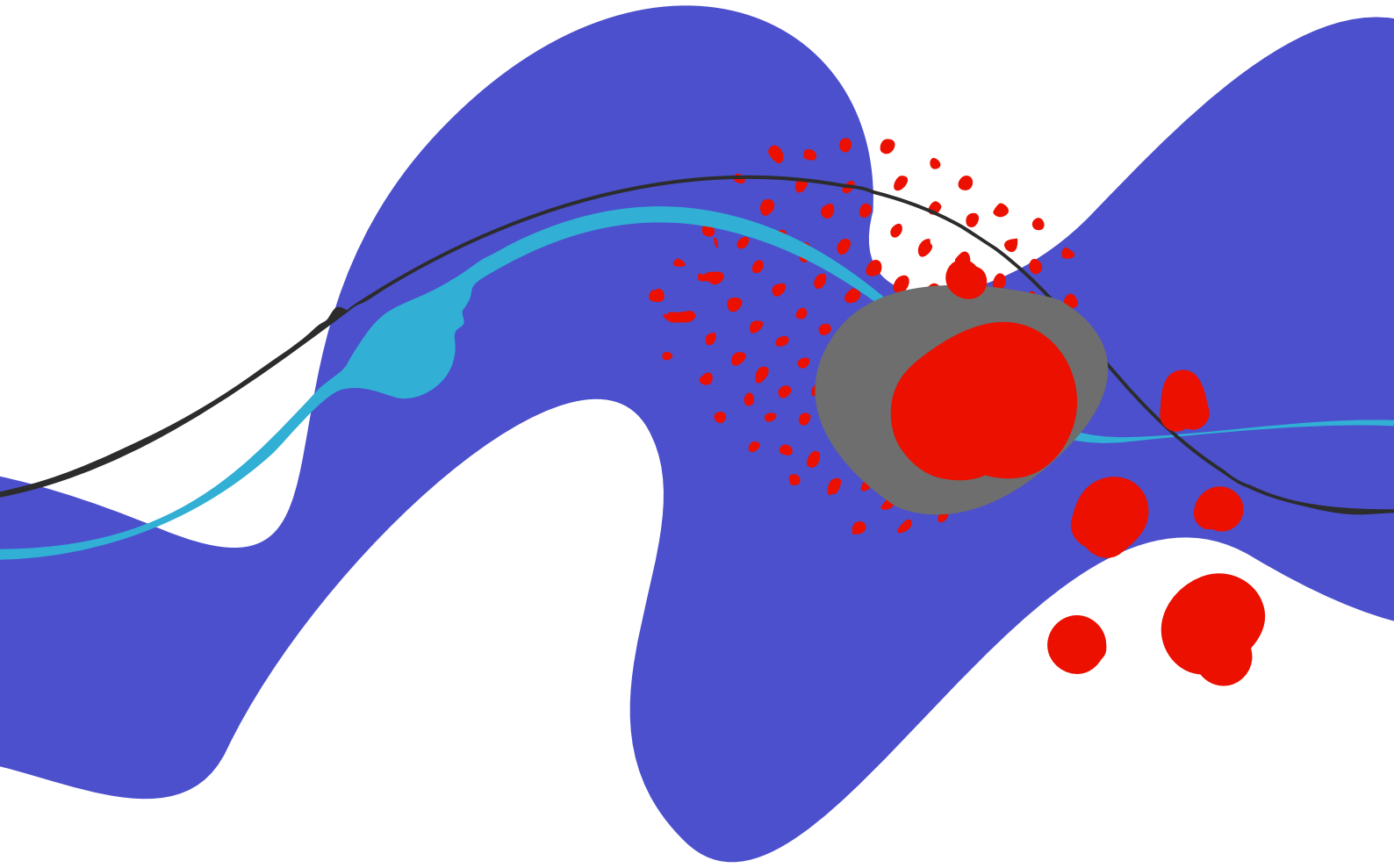
ARTICLE TECHNIQUE

Services de gestion des identités Adobe La sécurité



Sommaire

Sécurité Adobe	3
Services de gestion des identités Adobe	3
Types d'identité	4
Gestion des identités	5
Authentification et flux de données d'autorisation	7
Données d'identité	9
Présentation du programme de sécurité d'Adobe	12
Conclusion	17

Sécurité Adobe

Adobe® attache une grande importance à la sécurité des expériences digitales. Les pratiques de sécurité sont ancrées dans nos processus opérationnels et de développement logiciel, ainsi que dans nos outils, et les contrôles du programme Adobe Secure Product Lifecycle (SPLC) sont scrupuleusement appliqués par nos équipes pluridisciplinaires pour prévenir, détecter et résoudre rapidement les incidents. De plus, notre collaboration avec des partenaires, des chercheurs et des chercheuses, des instituts de recherche en sécurité et d'autres organisations sectorielles nous permet de mieux cerner les dernières menaces et vulnérabilités en date, et nous intégrons constamment des technologies et pratiques de sécurité renforcées aux produits et services que nous proposons.

Cet article technique décrit l'approche de « défense en profondeur » et les procédures de sécurité mises en œuvre par Adobe pour renforcer la sécurité de votre expérience des services de gestion des identités Adobe.

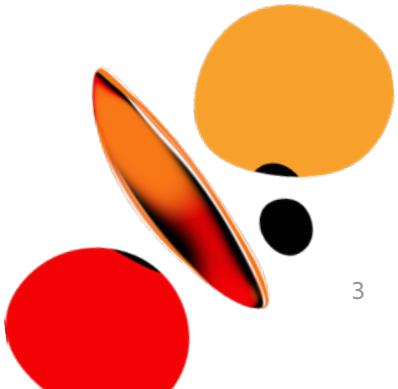
Services de gestion des identités Adobe

Gérant l'authentification des utilisateurs finaux et utilisatrices finales pour chaque solution Adobe, nos services de gestion des identités (IMS) incluent les trois (3) composants suivants :

- Le **service des identités Adobe**, qui gère l'authentification et la validation des utilisateurs finaux et des utilisatrices finales, y compris la fédération et l'exécution de l'authentification unique (SSO).
- **Adobe Admin Console**, qui permet de centraliser la gestion des droits d'accès Adobe pour toute l'entreprise. Adobe Admin Console permet de gérer les utilisateurs et les utilisatrices, les droits d'accès aux services cloud et aux applications pour ordinateur, la configuration de la fédération et la prévention des pertes de données.
- L'**API de gestion des utilisateurs et des utilisatrices Adobe (UMAPI)** permet aux entreprises de gérer leurs utilisateurs et leurs utilisatrices ainsi que les droits d'accès dans Adobe Admin Console au niveau de l'API.

Licences nominatives

La plateforme IMS Adobe gère les droits d'accès et les identifiants uniques, autrement dit les licences nominatives, ce qui permet aux utilisateurs finaux et aux utilisatrices finales de s'authentifier pour accéder à leurs applications pour ordinateur et services cloud Adobe.



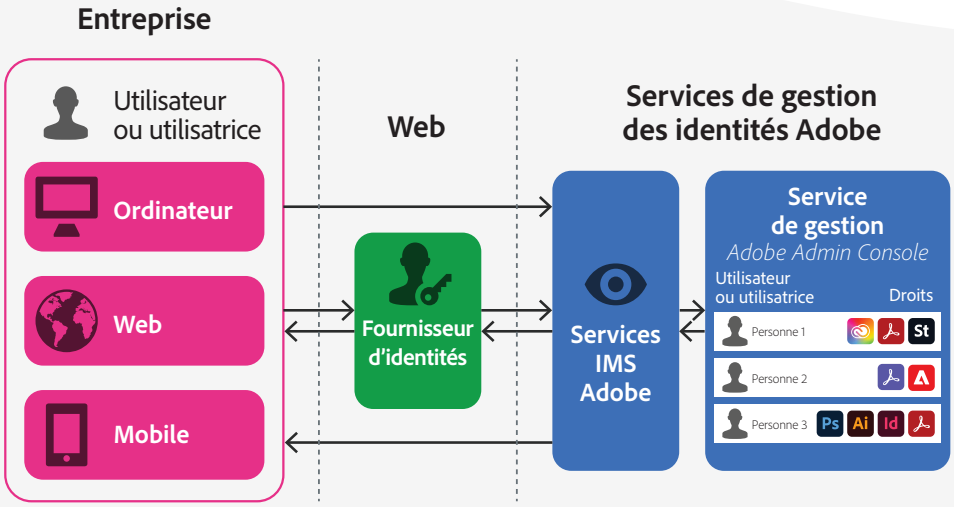


Figure 1 : Architecture des services de gestion des identités Adobe

La figure 1 ci-dessus illustre l'interaction d'une personne avec les services IMS Adobe via les licences nominatives. Dans l'exemple, cette personne a installé des applications Adobe sur son ordinateur ou ses appareils mobiles. Lorsqu'elle tente d'activer ou de lancer une application Adobe pour ordinateur ou appareil mobile ou d'accéder à un service cloud Adobe, l'appareil concerné communique avec les services IMS Adobe.

En fonction du type d'identité de la personne (voir la section suivante), les services IMS Adobe autorisent cette dernière à se connecter directement ou transmettent le contrôle au fournisseur d'identités de l'entreprise, qui procède à une authentification unique fédérée. Une fois l'authentification réussie, les services IMS Adobe vérifient les droits de la personne et effectuent l'action demandée. La personne peut alors utiliser le logiciel ou les services sur lesquels elle a des droits.

Types d'identité

Dans le cadre des déploiements en entreprise, Adobe prend en charge trois (3) types d'identité :

Hébergés par Adobe et gérés par l'entreprise, les **Business ID** sont destinés aux entreprises qui utilisent des adresses e-mail hors de leur domaine déclaré comme identifiants, ou à la clientèle qui n'a pas déclaré de domaines pour les identités. Adobe Business ID est l'option privilégiée par les entreprises qui font appel à des prestataires ou freelances ne possédant ni identifiant, ni adresse e-mail d'entreprise.

Avec **Enterprise ID**, les comptes sont hébergés par Adobe et administrés par l'entreprise. Ils sont créés par le service IT de l'entreprise cliente. L'entreprise détient et administre les comptes et toutes les ressources associées. Les comptes sont gérés via Adobe Admin Console et/ou l'UMAPI. Les gestionnaires de comptes peuvent définir des règles d'authentification, mais c'est Adobe qui gère l'authentification et les identifiants.

Federated ID est un compte administré par l'entreprise. Tous les profils d'identité sont fournis par un système de gestion des identités SSO et sont créés, détenus et contrôlés par le service IT. Adobe offre une intégration avec tous les fournisseurs d'identités compatibles SAML 2.0. Les comptes sont authentifiés via le fournisseur d'identités et autorisés via Adobe Admin Console. Le fournisseur d'identités de l'entreprise a la mainmise sur la configuration et l'application des règles d'authentification. Adobe gère aussi la connexion aux services Microsoft Azure Active Directory et Google Workspace Directory et la synchronisation avec ceux-ci via OpenID Connect pour les services d'identité fédérés.

La plupart des entreprises utilisent des Enterprise ID ou des Federated ID pour leurs effectifs, prestataires et freelances, à condition que l'adresse e-mail fasse partie des domaines déclarés de la société. Adobe recommande d'utiliser des Business ID si l'adresse e-mail des utilisateurs ou des utilisatrices n'utilise pas le domaine de l'entreprise. Pour plus d'informations, consultez la page d'aide Adobe sur les types d'identité.

Adobe déconseille le type d'identité Adobe ID pour les déploiements en entreprise. Il est en effet plus adapté à un usage individuel ou personnel.

Gestion des identités

Les entreprises clientes peuvent gérer les identités manuellement ou automatiquement.

Gestion manuelle des identités

Les personnes en charge de l'administration peuvent gérer manuellement les utilisateurs et les utilisatrices, soit individuellement en les ajoutant, en les supprimant ou en les modifiant une par une dans Adobe Admin Console, soit par lots en chargeant une liste au format CSV dans Adobe Admin Console.

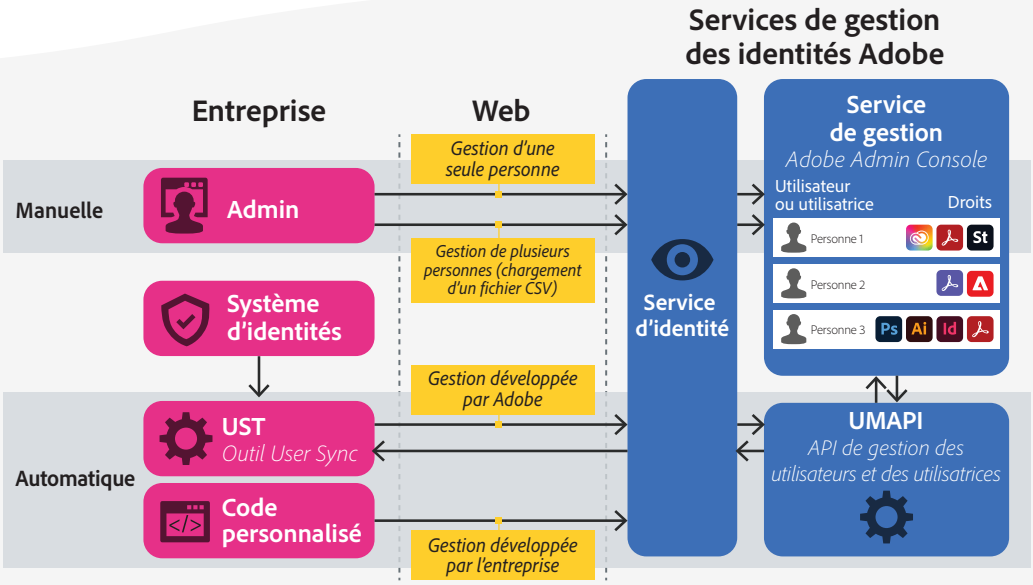


Figure 2 : Options de gestion des identités

Gestion automatique des identités

Si une personne en charge de l'administration souhaite gérer automatiquement les utilisateurs et les utilisatrices, elle peut opter pour l'une des trois (3) méthodes suivantes :

- Ajout, modification et suppression automatiques d'utilisateurs et utilisatrices via du code personnalisé avec l'**UMAPI**
- Synchronisation de l'ensemble des utilisateurs et des utilisatrices avec les services Microsoft Azure Active Directory et Google Workspace Directory à l'aide de la norme ouverte **SCIM (System for Cross-domain Identity Management)** pour la synchronisation dans le cloud
- Synchronisation de certaines personnes de l'annuaire d'entreprise, puis ajout aux groupes de licences appropriés ou suppression de ces derniers dans Adobe Admin Console à l'aide de **l'outil User Sync (UST)**, un ensemble de scripts Python développés et gérés par Adobe

Outil User Sync

L'outil UST lit les données d'identité de tous les groupes LDAP (Lightweight Directory Access Protocol) dans le service d'annuaire de l'entreprise (comme Microsoft Active Directory et les autres annuaires pris en charge par OpenID Connect) et effectue des appels REST sécurisés vers l'UMAPI pour créer, modifier ou supprimer des personnes sur les serveurs Adobe.

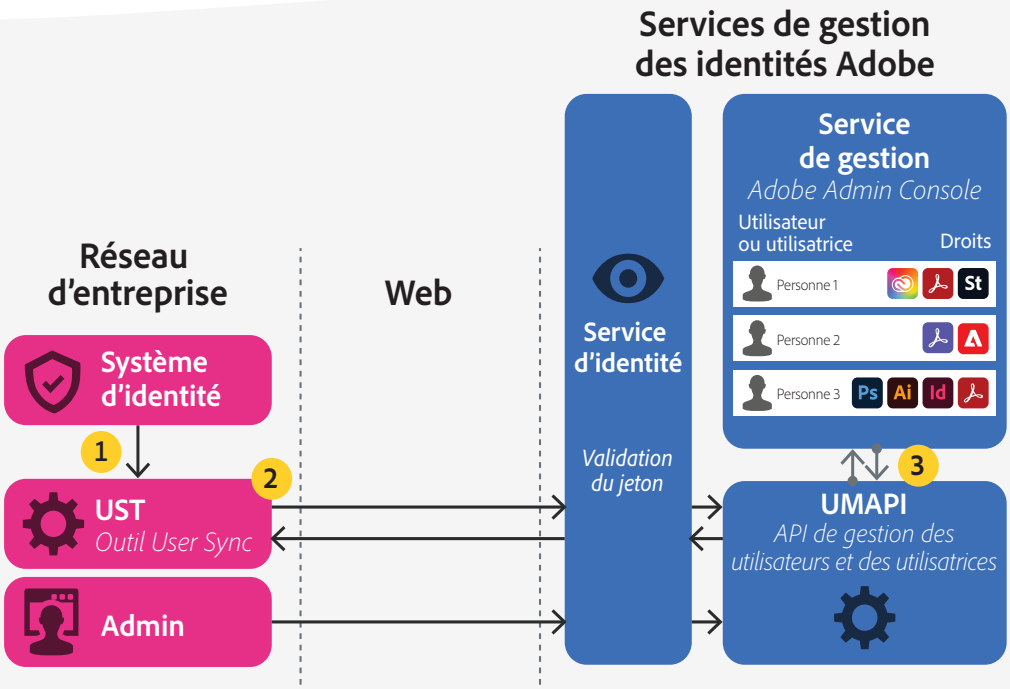


Figure 3 : L'outil User Sync (UST)

À chaque exécution, l'outil UST effectue les opérations suivantes :

1. Il demande les dossiers du personnel auprès des groupes au sein de l'annuaire de l'entreprise. Les groupes et la requête LDAP peuvent être personnalisés en fonction de l'environnement particulier de l'entreprise.
2. Il demande à Adobe Admin Console les utilisateurs et les utilisatrices actuelles et les configurations de produit correspondantes. Il se connecte à l'UMAPI via des appels REST sur HTTPS en utilisant un jeton d'accès vérifié et limité dans le temps généré par un jeton web JSON signé et codé.
3. Il détermine les utilisateurs et les utilisatrices à créer, supprimer ou modifier en fonction des règles définies dans les fichiers de configuration.
4. Il apporte les modifications nécessaires dans Adobe Admin Console via l'UMAPI, en octroyant les droits d'accès aux logiciels et services appropriés.

L'outil UST peut automatiquement synchroniser les droits Adobe des utilisateurs et des utilisatrices de l'entreprise avec leurs groupes dans le service d'annuaire. Par exemple, si une personne est ajoutée dans l'annuaire LDAP, lors de l'exécution suivante de l'outil UST, l'UMAPI extrait de l'annuaire les informations relatives à la personne et les ajoute au groupe approprié dans Adobe Admin Console. Si une personne est modifiée ou supprimée de l'annuaire LDAP, l'outil UST appelle l'UMAPI et effectue l'action appropriée dans Adobe Admin Console.

Pour plus de détails sur l'installation, l'enregistrement et l'exécution de l'outil UST, consultez la page d'aide Configuration de l'outil User Sync.

Des informations supplémentaires sur la gestion des utilisateurs et des utilisatrices sont disponibles sur la page d'aide Adobe Utilisateurs du portail Adobe Admin Console.

Authentification et flux de données d'autorisation

Adobe propose deux (2) méthodes d'authentification et d'autorisation :

L'authentification et l'autorisation sont interactives lorsqu'une personne se connecte expressément à une application pour ordinateur ou un service cloud Adobe et saisit ses informations dans une boîte de dialogue de l'interface. Le cas échéant, l'autorisation s'opère en toute transparence. Pour l'utilisateur ou l'utilisatrice, elle semble faire partie du processus d'authentification.

Adobe prend aussi en charge l'authentification multifactorielle (MFA), qui offre une couche de sécurité supplémentaire en imposant aux utilisateurs et aux utilisatrices de saisir des informations supplémentaires qu'elles seules connaissent après avoir été authentifiées via la vérification initiale en deux étapes dans l'interface. Adobe propose des règles d'application de l'authentification MFA pour les Adobe ID et les Business ID. Même en cas de déploiement MFA, l'autorisation s'opère en toute transparence. Pour l'utilisateur ou l'utilisatrice, elle semble faire partie du processus d'authentification.

L'authentification et l'autorisation sont automatiques une fois l'utilisateur ou l'utilisatrice authentifiée une première fois via l'authentification interactive. L'authentification automatique utilise un jeton d'identification unique, pour éviter à la personne de devoir se connecter une nouvelle fois pendant la session, et l'autorisation s'effectue également en toute transparence. À chaque interaction avec une application ou un service ne nécessitant pas expressément de se connecter, la personne concernée bénéficie de l'authentification automatique. Une fois la session terminée, les autorisations sont de nouveau contrôlées lors de la connexion suivante pour vérifier les droits d'accès.

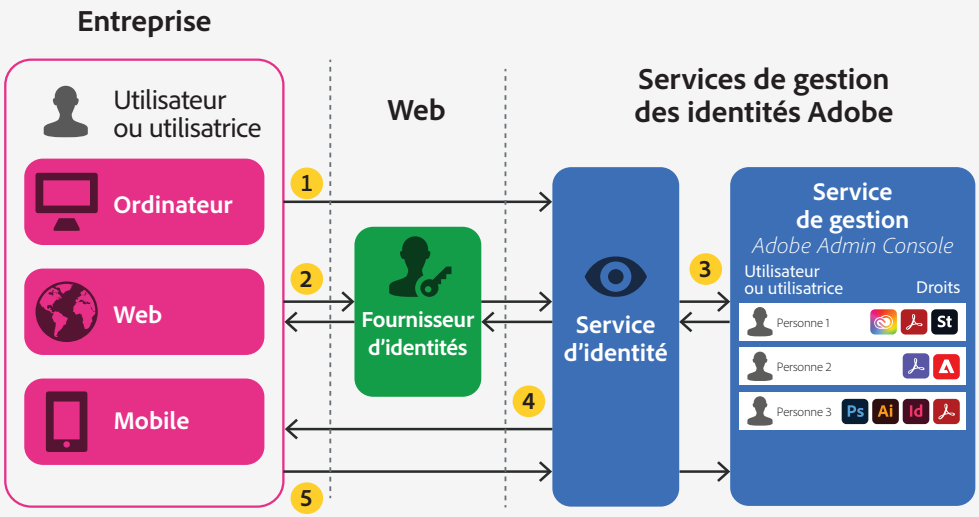


Figure 4 : Flux de données d'authentification Adobe

Si le flux de données d'authentification dépend du type d'identité, le processus d'authentification inclut généralement les étapes suivantes, chacune correspondant à un chiffre dans le diagramme ci-dessus :

1. La personne lance une application pour ordinateur ou demande l'accès à un service cloud Adobe pour la première fois. Si elle utilise un Business ID ou un Enterprise ID, elle se connecte via les services Adobe IMS.

2. Si l'entreprise utilise des Federated ID, lorsque la personne saisit son adresse e-mail ou simplement le nom de domaine (par exemple, @domainedelentreprise) dans le champ du nom d'utilisateur ou d'utilisatrice, les services Adobe IMS lancent une requête SAML. Celle-ci redirige la personne vers son fournisseur d'identités pour qu'elle se connecte à l'aide de ses identifiants d'entreprise.

3. Une fois la personne correctement authentifiée, les services Adobe IMS procèdent alors aux vérifications requises en matière de droits et d'application des règles, puis redirigent la personne vers le service cloud ou activent la licence applicative Adobe concernée.

4. Les services Adobe IMS stockent un jeton d'appareil sur l'ordinateur de la personne et s'en servent pour générer un jeton d'accès (semblable à un jeton de session d'application). Ensemble, ces deux jetons sont utilisés pour générer une licence signée pour l'application, qui est cryptée et stockée avec le jeton d'appareil dans les paramètres de la personne. Le jeton étant indépendant du système d'exploitation, en cas de redémarrage de la machine, aucune nouvelle authentification n'est nécessaire pour accéder à l'application ou au service cloud.

5. À ce stade, la personne peut utiliser simultanément toute application ou tout service cloud sans avoir à se réauthentifier manuellement dans chaque application (authentification automatique). En cas de lancement d'une autre application lors de la même session, les services Adobe IMS sont contactés et l'identifiant et le jeton de l'appareil sont échangés contre un jeton d'accès. Les règles et les droits sont vérifiés pendant le processus. Si pour une raison quelconque, les droits d'accès sont modifiés ou révoqués, les jetons d'accès et d'appareil perdent leur validité.

Adobe propose des règles d'administration facultatives qui limitent davantage la durée de validité des jetons d'accès en imposant une authentification plus fréquente. Ce système peut s'avérer utile pour certaines applications Adobe Experience Cloud. Adobe déconseille toutefois d'appliquer ces règles, sauf si l'entreprise a des exigences de sécurité particulières.

Données d'identité

Quelles données collectons-nous et pourquoi ?

Adobe collecte des données d'identité garantissant que chaque personne dispose d'un identifiant unique pour les vérifier dans le cadre de l'octroi de licences, et pour protéger par mot de passe ces droits et le contenu généré et stocké par la personne. Concernant les données d'identité, Adobe collecte les informations suivantes :

- **Nom d'utilisateur ou d'utilisatrice et domaine**. Il s'agit d'un identifiant de l'utilisateur ou de l'utilisatrice, généralement une adresse e-mail au format utilisateur@domaine. Pour les Business ID et les Enterprise ID, le nom complet de l'utilisateur ou de l'utilisatrice est requis pour la connexion aux applications et aux services cloud Adobe. Certaines entreprises utilisent des noms d'utilisateur ou d'utilisatrice qui ne correspondent pas à l'adresse e-mail (par exemple, prénomnom d'un côté, et utilisateur@domaine de l'autre). Le cas échéant, le choix revient à l'entreprise. Pour les Federated ID, l'adresse e-mail complète ou seulement la partie @domaine est requise pour transmettre le contrôle au fournisseur d'identités adéquat.

- **UID (Federated ID uniquement)**. Cet identifiant unique est associé à la personne (il s'agit généralement de l'adresse e-mail). Adobe utilise l'UID comme clé du fournisseur d'identités pour rechercher la personne dans les services IMS.

- **Mot de passe (Business ID et Enterprise ID uniquement)**. Les mots de passe sont hachés conformément aux bonnes pratiques du secteur avant d'être stockés. Adobe ne conserve jamais de copie d'un mot de passe dans un format susceptible d'être décrypté en texte simple.

- **Date de naissance (Adobe ID uniquement)**. En vertu de la loi COPPA (Children's Online Privacy Protection Act) et du Règlement général sur la protection des données (RGPD), cette information est obligatoire pour vérifier l'âge d'une personne qui tente d'accéder à certains sites web.

- **Code pays**. Les codes pays ISO Alpha-2 et ISO Alpha-3 de la personne sont recueillis lors de la création du profil d'identité. En général, Adobe utilise le code pays pour déterminer l'emplacement de stockage géographique du contenu créé par l'utilisateur ou l'utilisatrice. L'emplacement des Enterprise ID et des Federated ID est choisi par l'entreprise.

- **Nom et prénom**. Ces informations sont recueillies lors de la création du profil d'identité. Pour les Enterprise ID et les Federated ID, les champs UID, Code pays, Nom et Prénom peuvent être configurés par la personne en charge de l'administration au sein du service IT lors de la création des comptes utilisateur ou utilisatrice. Les personnes en charge de l'administration peuvent aussi décider du nombre d'informations sur les utilisateurs et les utilisatrices incluses dans ces champs.

Où stockons-nous vos données d'identité ?

Quelle que soit la zone géographique de la clientèle, toutes les données d'identité sont stockées chez des fournisseurs d'infrastructure cloud multirégionaux à équilibrage de charge. Ceux-ci possèdent des centres de données en Amérique du Nord (Oregon et Virginie), en Europe (Irlande) et dans la zone Asie-Pacifique (Singapour). Les données d'identité sont répliquées dans tous les centres de données pour plus de fiabilité.

Comment protégeons-nous vos données d'identité ?

Toutes les données d'identité stockées sont protégées via un cryptage AES 256 bits conformément à Adobe CCF (Common Controls Framework) et à nos règlements internes en matière de cryptage et de stockage des données sensibles.

Pendant combien de temps conservons-nous vos données d'identité ?

Le contenu est répliqué dans chaque centre de données, dans d'autres centres de la zone géographique ainsi que dans des centres couvrant plusieurs zones géographiques, à des fins d'équilibrage de charge et de redondance. Les données d'identité sont sauvegardées quotidiennement dans les centres de données. Ces sauvegardes sont conservées pendant sept (7) jours. De plus, Adobe respecte les lois en vigueur en matière de transfert de données d'un pays à l'autre.

La création, la détention et le contrôle d'un compte Adobe ID sont à la charge de la personne concernée, qui contrôle donc le cycle de vie du compte. Néanmoins, la règle de conservation stipulée dans la norme CPIR (Consumer Personal Information Retention) prévoit que les Adobe ID et Business ID inactifs pendant plus de quatre (4) ans ne sont pas conservés. Adobe désactive le compte Adobe ID et supprime les informations personnelles, le mot de passe haché et les données de paiement correspondantes sur demande de la personne concernée ou après 48 mois consécutifs d'inactivité.

Pour les Enterprise ID et les Federated ID, le calendrier de suppression des comptes est déterminé par l'entreprise cliente et peut être contrôlé via Adobe Admin Console. Lorsqu'une entreprise ne souhaite plus qu'un Enterprise ID ou un Federated ID soit associé à son compte, une personne en charge de l'administration peut le supprimer via Adobe Admin Console. Pour plus d'informations, consultez la page d'aide Utilisateurs du portail Adobe Admin Console.

Comment gérons-nous les journaux d'évènements ?

Adobe enregistre dans des journaux d'évènements les actions suivantes des utilisateurs et des utilisatrices :

- Activation d'une application ou d'un service Adobe
- Connexion à une application ou à un service Adobe
- Ouverture d'une application Adobe sur l'ordinateur ou l'appareil mobile d'une personne
- Utilisation de l'espace de stockage ou des services cloud

Les données de journaux collectées peuvent inclure l'identifiant, l'adresse e-mail et l'adresse IP de la personne, ainsi que des données de suivi des évènements. Adobe peut également enregistrer des données analytiques liées à l'utilisation de l'application et des services. Les utilisateurs et les utilisatrices peuvent refuser la collecte de données analytiques à tout moment.

Qui peut accéder à vos données d'identité ?

Conformément à la certification ISO 27001 d'Adobe, seul le personnel autorisé d'Adobe a accès aux données d'identité. De plus, les accès sont accordés sur demande et en respectant le principe de privilège minimal. Les données enregistrées dans des journaux par les services Adobe IMS sont considérées comme protégées par un « privilège maximal » (conformément à la norme de classification et de traitement des données appliquée par Adobe). Leur accès par le personnel d'Adobe est encore plus restreint.

Présentation du programme de sécurité d'Adobe

Le programme de sécurité intégré d'Adobe comprend cinq (5) centres d'excellence. Chacun d'entre eux itère et perfectionne constamment les méthodes de détection et de prévention des risques, en tirant parti de technologies nouvelles et émergentes comme l'automatisation, l'IA et le machine learning.

Figure 5 : les cinq centres d'excellence du programme de sécurité

Les centres d'excellence du programme de sécurité d'Adobe s'articulent autour des thèmes suivants :

- la **sécurité applicative**, qui couvre la sécurité de la programmation des produits, la recherche sur les menaces et le programme bug bounty ;
- la **sécurité opérationnelle**, qui contribue à surveiller et protéger les systèmes, réseaux et systèmes de production dans le cloud ;
- la **sécurité de l'entreprise**, qui se concentre sur l'authentification et l'accès sécurisé à l'environnement interne d'Adobe ;
- la **conformité**, qui regroupe la supervision du modèle de gouvernance de la sécurité, les programmes d'audit et de conformité et l'analyse des risques ;
- la **résolution des incidents**, qui incombe au centre des opérations de sécurité et aux spécialistes de la limitation des menaces, dont les activités s'opèrent 24 h/24, 7 j/7.

Dans le cadre de l'engagement d'Adobe en faveur de la sécurité des produits et services, les centres d'excellence sont placés sous l'autorité de la personne responsable de la sécurité (CSO). Celle-ci coordonne l'ensemble des efforts de sécurité et oriente la vision d'Adobe concernant les évolutions à venir dans ce domaine.

Pôle de sécurité d'Adobe

S'appuyant sur un processus décisionnel transparent, responsable et éclairé, le pôle de sécurité d'Adobe rassemble tous les services de sécurité en vertu d'un modèle de gouvernance unique. Au niveau de la direction, le ou la CSO collabore étroitement avec le ou la DSI et le ou la responsable de la confidentialité (CPO) pour garantir la cohérence de la stratégie et des opérations de sécurité.

Outre les centres d'excellence décrits ci-dessus, Adobe implique différents services (juridique, confidentialité, marketing et relations publiques) dans les activités du pôle sécurité afin de favoriser la transparence et la responsabilité dans toutes les décisions ayant trait à la sécurité.

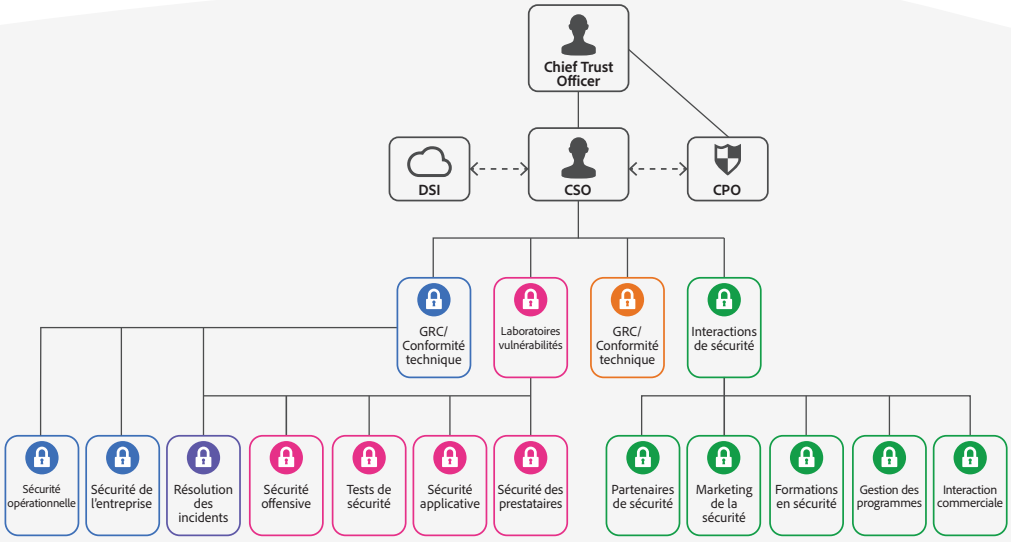


Figure 6 : pôle de sécurité d'Adobe

Dans le cadre de la culture de sécurité de l'entreprise, chaque collaborateur et collaboratrice doit suivre une formation de sensibilisation à la sécurité. Celle-ci est sanctionnée par un examen initial et fait l'objet de contrôles annuels pour garantir que l'ensemble du personnel contribue à protéger les ressources de l'entreprise, ainsi que les données de la clientèle et des équipes. À l'embauche, les effectifs techniques (notamment les équipes chargées de l'ingénierie et des opérations techniques) sont automatiquement inscrits à un programme de formation approfondie. Celui-ci est adapté en fonction du poste.

Découvrez en détail la culture de la sécurité et les programmes de formation d'Adobe dans cet article technique.

Adobe SPLC

Toutes les mesures de sécurité prises par Adobe reposent sur le programme Secure Product Lifecycle (SPLC). Celui-ci est intégré à plusieurs étapes du cycle de vie du produit, de la conception au déploiement en passant par le développement, les tests et l'assurance qualité. Regroupant plusieurs centaines d'activités de sécurité liées aux pratiques, aux processus et outils de développement logiciel, Adobe SPLC a mis en place des processus clairs et reproductibles pour aider les équipes de développement à intégrer la sécurité aux produits et services. De plus, le programme évolue constamment pour incorporer les bonnes pratiques du secteur les plus récentes.

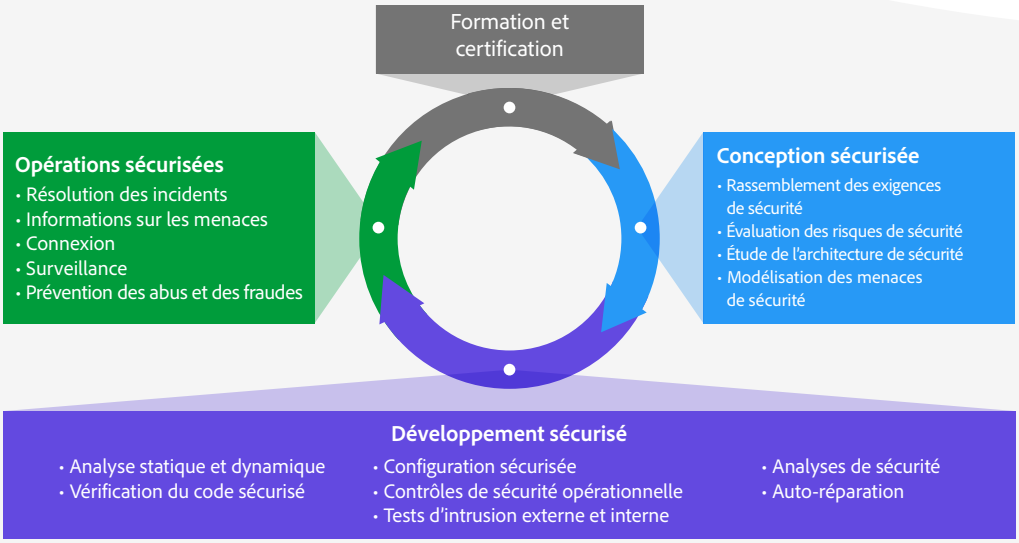


Figure 7 : Adobe SPLC

Adobe a publié une norme sur la sécurité du cycle de vie des produits. Celle-ci peut être consultée sur demande. Pour plus d'informations sur les composantes d'Adobe SPLC, consultez la présentation de la sécurité applicative d'Adobe.

Sécurité applicative

Le développement de nos applications selon une méthode sécurisée par défaut repose sur la pile de sécurité applicative Adobe. Associant, d'une part, des processus clairs et reproductibles, découlant d'études validées et de notre vaste expérience et, d'autre part, des technologies d'automatisation garantes de l'application systématique de contrôles de sécurité, la pile de sécurité applicative Adobe contribue à renforcer l'efficacité du développement et à limiter le risque d'erreurs de sécurité. Nos équipes de développement utilisent des blocs de code sécurisés, ayant fait l'objet de tests et d'une validation préalable. Ainsi, elles n'ont pas besoin de programmer de A à Z les patrons et blocs courants et peuvent se concentrer sur leur domaine d'expertise, avec la certitude que leur code est sûr. En conjonction avec les tests, les outils spécialisés et le suivi, la pile de sécurité applicative Adobe aide les spécialistes du développement à créer du code sécurisé par défaut.

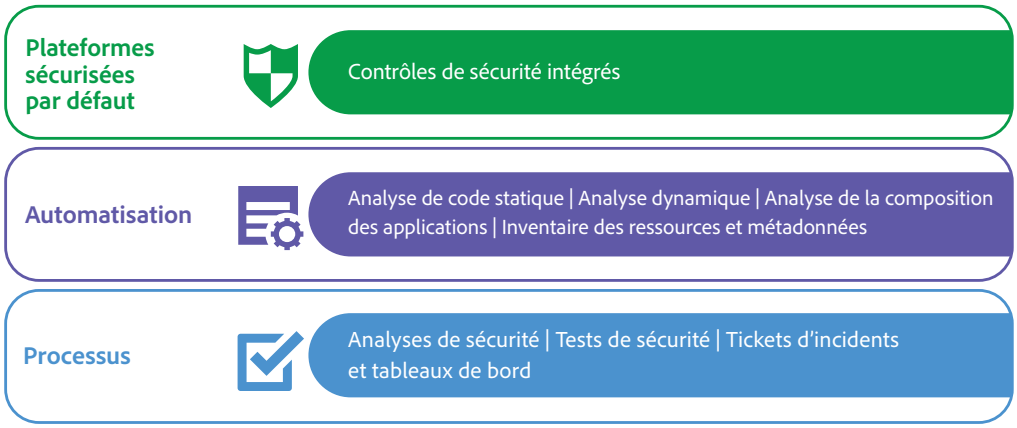


Figure 8 : la pile de sécurité applicative d'Adobe

Adobe a également publié plusieurs normes sur la sécurité applicative, notamment celles relatives à son utilisation de l'infrastructure cloud publique AWS (Amazon Web Services) et Microsoft Azure. Ces normes sont disponibles pour consultation sur demande. Pour en savoir plus sur les méthodes et les processus de sécurité applicative d'Adobe, consultez la présentation de la sécurité applicative d'Adobe.

Sécurité opérationnelle

Pour s'assurer que tous les produits et services Adobe sont conçus dès le départ en tenant compte des bonnes pratiques de sécurité, l'équipe en charge de la sécurité opérationnelle a créé la pile OSS (Operational Security Stack). Cette suite d'outils aide les équipes de développement et d'ingénierie à renforcer leurs pratiques de sécurité et à réduire les risques pesant sur Adobe et sa clientèle, tout en contribuant au respect des frameworks de conformité, de confidentialité et de gouvernance.

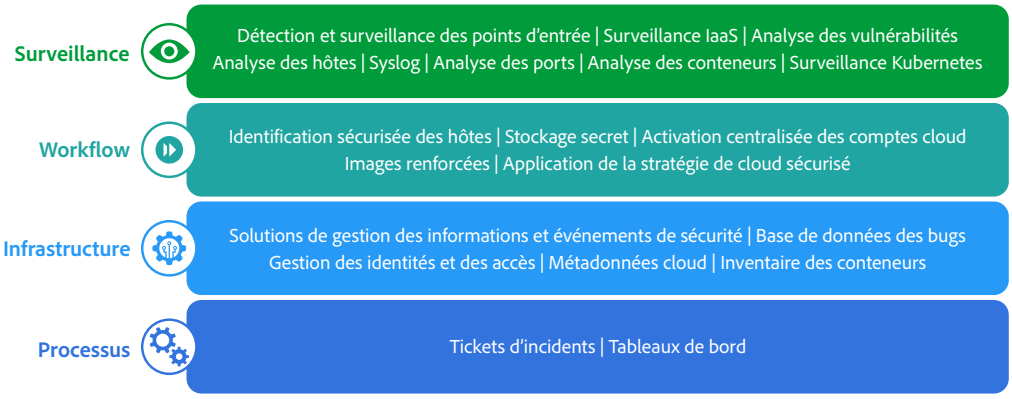


Figure 9 : la pile de sécurité opérationnelle d'Adobe

Adobe a publié plusieurs normes sur ses opérations cloud. Ces normes peuvent être consultées sur demande. Pour une description détaillée de la pile de sécurité opérationnelle d'Adobe et des outils utilisés au sein de l'entreprise, consultez la présentation de la sécurité opérationnelle d'Adobe.

Sécurité de l'entreprise

Outre la protection de ses produits et services ainsi que de ses opérations d'hébergement dans le cloud, Adobe applique divers contrôles pour garantir la sécurité de ses réseaux et systèmes internes, de ses locaux, de son personnel et des données de sa clientèle.

Pour plus d'informations sur ces contrôles de sécurité et sur les normes élaborées à cette fin, consultez la présentation de la sécurité de l'entreprise Adobe.

Conformité Adobe

Tous les produits et services Adobe respectent Adobe CCF (Common Controls Framework), un ensemble d'activités de sécurité et de contrôles de conformité mis en œuvre par nos équipes en charge des opérations produits et, à divers niveaux, par nos équipes responsables de l'infrastructure et des applications. Adobe s'appuie autant que possible sur des processus d'automatisation de pointe pour signaler à ses équipes les situations qui présentent un risque de non-conformité, afin de garantir une correction et un réalignement rapides.

Les produits et services Adobe sont soit conformes à la législation en vigueur, soit conçus de telle sorte que la clientèle qui les utilise se conforme aux obligations légales lui incombant au titre du recours à des prestataires de services. La clientèle garde le contrôle de ses documents, de ses données et de ses workflows, et peut choisir la meilleure façon de se conformer aux règlementations locales ou régionales, comme le Règlement général sur la protection des données (RGPD) dans l'UE.

Par ailleurs, Adobe a élaboré une formation et des normes sur la conformité. Celles-ci sont disponibles sur demande. Pour plus d'informations sur Adobe CCF et les certifications essentielles, consultez la liste des certifications, normes et règlementations de conformité gérées par Adobe.

Résolution des incidents

Adobe met un point d'honneur à garantir la souplesse et la précision des processus de gestion des risques et des vulnérabilités, de résolution des incidents et de limitation des menaces. Nous surveillons en permanence les menaces, partageons nos informations avec les spécialistes de la sécurité dans le monde entier, résolvons rapidement les incidents et transmettons ces informations à nos équipes de développement afin d'atteindre un niveau de sécurité maximal pour tous les produits et services Adobe.

Nous avons également élaboré des normes internes en matière de résolution des incidents et de gestion des vulnérabilités. Celles-ci peuvent être consultées sur demande.

Pour en savoir plus sur le processus de résolution et de notification des incidents mis en œuvre par Adobe, consultez la présentation du programme de résolution des incidents d'Adobe.

Continuité d'activité et reprise sur incident

Ce programme comprend un plan de continuité d'activité et un plan de reprise sur incident propre à chaque produit, qui permettent tous deux d'assurer la disponibilité et la distribution en continu des produits et services Adobe. Certifié ISO 22301, notre programme de continuité d'activité et de reprise sur incident améliore notre capacité à réagir aux évènements inattendus et à en limiter les répercussions. Pour plus d'informations, consultez la présentation du programme de continuité d'activité et de reprise sur incident d'Adobe.

Conclusion

L'approche proactive d'Adobe en matière de sécurité et les procédures rigoureuses décrites dans ce document contribuent à assurer la sécurité d'Adobe Sign et de vos données confidentielles. Chez Adobe, nous prenons très au sérieux la sécurité de vos expériences digitales et surveillons en permanence un environnement où les menaces évoluent constamment, afin de conserver une longueur d'avance sur les activités malveillantes et de garantir la sécurité des données de notre clientèle.

Pour en savoir plus sur la sécurité Adobe, consultez le Centre de données Adobe.

Adobe

12/22