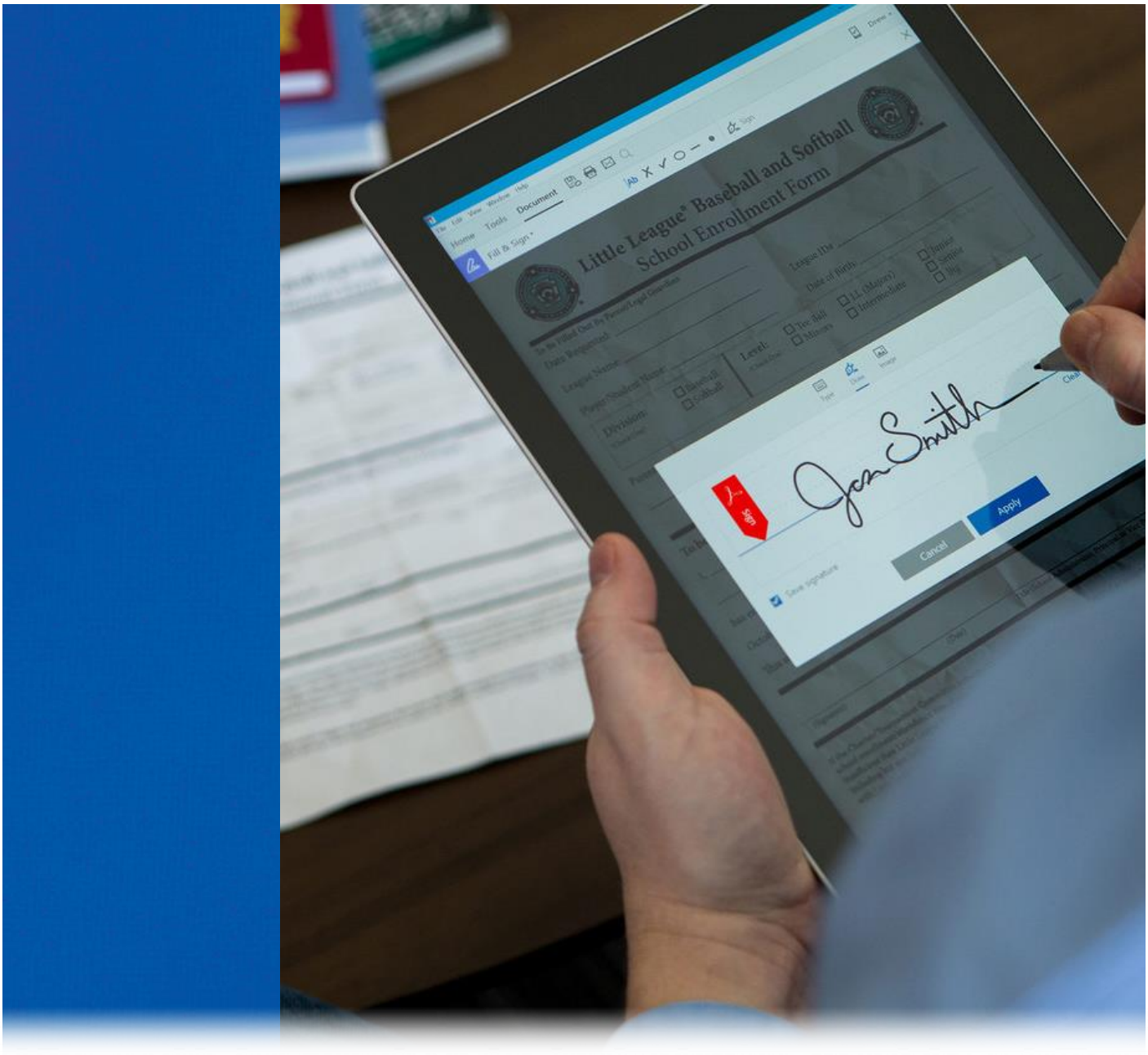

ADOBE SIGN

Conformité avec la législation européenne en matière de signatures électroniques

Décembre 2016

DLA PIPER

Adobe

TABLE DES MATIÈRES

1 INTRODUCTION

Ce document évalue l'efficacité juridique de la solution Adobe Sign eu égard aux exigences européennes applicables aux signatures électroniques. Dans la première partie de ce document, nous donnons un aperçu du cadre juridique pertinent. Nous décrivons ensuite brièvement la portée, les principaux concepts et les conséquences juridiques du Règlement 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, (ci-après **"Règlement eIDAS"** ou **"Règlement"**) qui est l'instrument principal qui gouverne la validité des signatures électroniques dans l'UE. Nous analysons également plus en détail les questions clés relatives à la validité et le caractère exécutoire des contrats signés de manière électronique.

Dans la deuxième partie, ce document blanc décrit les caractéristiques essentielles d'Adobe Sign et examine ces caractéristiques eu égard aux exigences légales afin d'évaluer le caractère juridiquement contraignant des signatures électroniques produites par le biais de la solution Adobe Sign.

Nous en concluons que lorsque les paramètres d'utilisateur appropriés sont sélectionnés, d'un point de vue juridique, Adobe Sign est un outil fiable et sécurisé qui permet de produire des signatures électroniques qui se conforment ou même dépassent les exigences de la signature électronique telle que définie à l'Article 3.10 du Règlement eIDAS.

De plus, nous pensons qu'il existe des arguments pour affirmer qu'Adobe Sign, sans utiliser la technologie de signature numérique, est en mesure de produire des signatures électroniques avancées telles que définies à l'Article 3.11 du Règlement eIDAS.

Par ailleurs, nous observons qu'Adobe Sign contient également une option pour utiliser la technologie de signature numérique, notamment les signatures électroniques avancées basées sur des certificats numériques et les signatures électroniques qualifiées telles que définies à l'Article 3.12 du Règlement eIDAS. Par conséquent, si cette option est activée par l'utilisateur, Adobe Sign peut être considéré comme un outil facile d'utilisation pour les entreprises afin de permettre et de faciliter le processus de production de signatures électroniques avancées et qualifiées.

Compte tenu des considérations qui précèdent, Adobe Sign, s'il est configuré en conséquence, peut être considéré comme une solution de signature électronique fiable qui permet de gérer tout un processus de signature conforme à tous les types de signatures électroniques établies en vertu du Règlement eIDAS. Adobe Sign permet en particulier aux utilisateurs de configurer et d'établir un flux de travail en fonction de la conformité particulière de l'utilisateur, de l'industrie et du profil des risques.

2 CADRE RÉGLEMENTAIRE

2.1 Règlement eIDAS

eSign Directive – Jusqu'il y a quelques mois, l'utilisation des signatures électroniques dans l'UE était gouvernée par la Directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques

(ci-après Directive eSign). L'harmonisation apportée par cette Directive eSign était imparfaite et a engendré un manque d'interopérabilité entre les solutions de signature électronique dans les différents États membres de l'UE et, par conséquent, a conduit à la fragmentation du marché. Bien que la Directive eSign précise les effets juridiques des signatures électroniques, elle ne garantit pas que la reconnaissance d'une signature électronique dans un État membre de l'UE implique nécessairement son acceptation dans un autre État membre de l'UE. Il en résultait que l'acceptation des signatures électroniques utilisées dans les transactions électroniques transfrontalières était incertaine. En outre, la Directive eSign n'est plus adaptée aux solutions de plus en plus innovantes qui permettent d'indiquer qu'une personne a également approuvé le contenu d'un document ou d'un contrat électronique.

Afin de stimuler l'utilisation des signatures électroniques et d'autres services de confiance pour les transactions électroniques et de contribuer à la création d'un marché unique numérique dans l'UE, le législateur européen a adopté le Règlement eIDAS en juillet 2014. La plupart des dispositions du Règlement eIDAS ne seront applicables qu'à partir du 1er juillet 2016. Alors que le Règlement eIDAS a abrogé la directive susmentionnée sur les signatures électroniques, il se fonde, clarifie et élargit les principes qui y figurent.

Règlement eIDAS – Le législateur européen ayant choisi un règlement (directement applicable dans tous les Etats membres de l'UE) au lieu de réviser la Directive eSign (qui aurait dû être transposée dans les législations nationales des Etats membres), les entreprises ne seront plus confrontées aux différentes législations nationales applicables mais devront se conformer à un ensemble de règles, ce qui réduira significativement le risque des questions d'interprétation. Bien que le Règlement eIDAS vise à garantir l'efficacité juridique des signatures électroniques et sa recevabilité comme preuve dans le cadre de procédures judiciaires, tout comme son prédécesseur, à savoir la Directive eSign, le Règlement eDIAS ne régit aucun aspect relatif à la conclusion ou à la validité des contrats (électroniques) (voir section 2.2 ci-dessous).

Le Règlement eIDAS fait une distinction entre les signatures électroniques, les signatures électroniques avancées et les signatures électroniques qualifiées.

2.1.1 Signatures électroniques standards

Large définition – Le Règlement eIDAS propose une large définition de la 'signature électronique' standard sans aucune référence à une technologie particulière. Une telle 'signature électronique' est définie comme des données sous forme électronique qui sont jointes ou associées logiquement à d'autres données sous forme électronique et qui sont utilisées par le signataire pour signer.

Dans son Considérant 26, le Règlement eIDAS précise qu'en raison de la rapidité de l'évolution technologique, il conviendrait de consacrer une approche qui se veut ouverte à l'innovation. Le Considérant 27 précise, en outre, que le Règlement eIDAS doit être neutre sur le plan technologique et que les effets juridiques qu'il confère doivent pouvoir être obtenus par tout moyen technique (pour autant que les exigences du Règlement soient satisfaites). Les trois critères nécessaires pour qualifier la signature électronique standard sont: (i) l'existence de 'données sous forme électronique', (ii) 'jointes ou associées logiquement à d'autres données sous forme électronique' et (iii) 'utilisées par le signataire pour signer'. Ces critères ne sont pas davantage définis ni expliqués dans le Règlement

eIDAS et laissent donc place à l'interprétation mais également à l'innovation technologique. En pratique, cela signifie que de nombreux outils électroniques permettant de capturer l'intention du signataire d'approuver le contenu d'un document peuvent être considérés comme une signature électronique. Il peut s'agir entre autres d'un code PIN, d'un mot de passe, d'une signature scannée, d'une signature de cryptographie symétrique ou de clé publique et d'une signature biométrique.

Effet juridique – Conformément à l'Article 25.1 du Règlement eIDAS, une signature électronique standard ne peut se voir refuser l'effet juridique et la recevabilité comme preuve dans le cadre de procédures judiciaires uniquement au motif qu'elle est sous forme électronique ou qu'elle ne satisfait pas aux exigences des signatures électroniques qualifiées. Bien que les États membres de l'UE restent libres de définir les effets juridiques des signatures électroniques standards, l'Article 25.1 du Règlement eIDAS a pour effet de ne pas autoriser les États membres de l'UE à rédiger ou à maintenir une législation, ni à approuver ou autoriser des règles nationales visant à refuser l'utilisation d'outils de signatures électroniques seulement sur la base de leur format électronique ou de leur nature non-qualifiée.

Le fait qu'une signature électronique standard ne puisse se voir refuser l'effet juridique et la recevabilité comme preuve sur la base de certaines caractéristiques techniques ne signifie toutefois pas qu'elle recevrait le même traitement juridique qu'une signature manuscrite. Cela ne sera le cas que si c'est prévu expressément dans des lois particulières. Par ailleurs, cela n'affecte pas les règles nationales concernant l'appréciation libre des éléments de preuve par les tribunaux.

Une signature électronique standard ne peut se voir refuser l'effet juridique et la recevabilité comme preuve dans les procédures judiciaires uniquement pour les motifs qu'elle est sous forme électronique et ne répond pas aux exigences applicables aux signatures électroniques qualifiées.

2.1.2 Signatures électroniques avancées

Quatre critères – Une 'signature électronique avancée' est définie par l'Article 3.10 du Règlement eIDAS comme une signature électronique standard qui satisfait aux exigences de l'Article 26 du Règlement eIDAS, notamment: a) elle est liée au signataire de manière univoque; b) elle est en mesure d'identifier le signataire; c) elle est créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif; et d) elle est liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Bien que la définition juridique d'une signature électronique avancée ait été formulée de manière neutre sur le plan technologique, ce concept est généralement interprété comme se référant principalement aux signatures électroniques fondées sur la technologie de signature numérique. En d'autres termes, cela signifie les signatures électroniques qui utilisent la cryptographie à clé publique. Selon cette interprétation, une signature électronique avancée doit être considérée comme un fichier numérique contenant une empreinte du document obtenu par encodage avec la clé privée du

signataire. La signature électronique avancée peut par conséquent être vérifiée avec la clé publique correspondante du signataire. Un certificat numérique correspondant, notamment une attestation électronique qui lie les données pour valider la signature à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne, confirme le signataire en tant que propriétaire de sa clé publique.

Signatures à distance – La définition technologiquement neutre de la signature électronique avancée n'exclut cependant pas qu'une quelconque autre technologie permettrait de produire des signatures électroniques avancées, à condition bien sûr que les quatre conditions susmentionnées soient satisfaites. D'une part, les Considérants 26 et 27 confirment que le Règlement eIDAS est ou devrait supporter l'innovation et que les effets juridiques que le Règlement eIDAS octroie devraient être réalisables par le biais de tous moyens techniques. D'autre part, le Considérant 52 ouvre la voie à l'utilisation juridiquement légale des solutions de signature électronique basées sur le cloud. Ce Considérant reconnaît que la création de signatures électroniques à distance, dans le cadre de signature électronique gérée par un prestataire de services de confiance pour le compte du signataire, est destinée à accroître. À cet égard, il est encore précisé que ces signatures électroniques devraient bénéficier de la même reconnaissance juridique que les signatures électroniques créées dans un cadre entièrement géré par les utilisateurs, à condition que le fournisseur de services de signature électronique à distance mette en place des procédures de sécurité spécifiques de gestion et d'administration et utilise des systèmes et des produits dignes de confiance afin de garantir que le cadre de création de signature électronique est fiable et est utilisé sous le contrôle exclusif du signataire. Étant donné la formulation générale de ce Considérant, on peut soutenir qu'un signataire peut conserver sa clé privée dans le cloud ou même utiliser une solution de signature électronique basée sur le cloud qui ne nécessite aucune clé de signataire.

Le Règlement eIDAS ne confère pas à la signature électronique avancée des effets juridiques spécifiques différents de ceux d'une signature électronique standard. Le concept est cependant utilisé comme élément essentiel pour définir la signature électronique qualifiée, qui est une signature électronique avancée qui satisfait à un certain nombre d'exigences légales supplémentaires (voir section 2.1.3 ci-dessous).

Niveau de confiance augmenté – La principale différence entre les signatures électroniques standards et les signatures électroniques avancées est toutefois que la sécurité technique d'une signature électronique avancée (souvent une signature électronique basée sur un certificat numérique) est généralement considérée comme supérieure à certaines signatures électroniques standards juridiquement acceptées, tel un code PIN ou une signature scannée jointe à un document. En général, les signatures électroniques avancées sont donc considérées comme plus fiables et les tribunaux leur confèrent une force probante plus importante. Cependant, d'un point de vue juridique, la méthode de technique utilisée n'est qu'un seul élément pris en compte à la discrétion des tribunaux. Par conséquent, dans un cas particulier, la fiabilité d'une signature électronique spécifique basée sur un certificat numérique pourrait être mise en doute, alors que dans un autre cas, un tribunal pourrait considérer qu'un code PIN fournit une preuve suffisante.

Malgré qu'aucun effet juridique spécifique ne soit attribué à une signature électronique avancée, elle est généralement considérée comme plus fiable et a une force probante plus importante devant un tribunal. En outre, le Règlement eIDAS semble laisser une place aux signatures électroniques qui ne sont pas fondées sur un certificat numérique pour qu'elles soient considérées comme une signature électronique avancée.

2.1.3 Signatures électroniques qualifiées

Équivalent à la signature manuscrite – Une 'signature électronique qualifiée' est définie à l'Article 3.12 du Règlement eIDAS comme une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifiée, et qui repose sur un certificat qualifié de signature électronique.

Un principe clé du Règlement eIDAS est que, conformément à son Article 25.2, une signature électronique qualifiée est automatiquement équivalente à une signature manuscrite et produit des effets juridiques équivalents. L'Article 25.3 du Règlement eIDAS stipule, en outre, qu'une signature électronique qualifiée reposant sur un certificat qualifié délivré dans un État membre de l'UE doit être reconnue comme une signature électronique qualifiée dans tous les autres États membres de l'UE. Ainsi, l'Article 25.3 du Règlement eIDAS remédie au manque d'interopérabilité qui affectait la Directive 1999/93/EC sur les signatures électroniques et permet des transactions électroniques transfrontalières sûres et harmonieuses en renforçant la reconnaissance juridique des signatures électroniques qualifiées à travers les États membres de l'UE.

Large ensemble de critères – Pour être considérée comme une signature électronique qualifiée, la signature électronique doit être basée sur un certificat qualifié. Un certificat 'qualifié' est un certificat numérique qui doit contenir les informations spécifiques énoncées à l'Annexe I du Règlement eIDAS et être délivré par un prestataire de services de confiance qualifié (après avoir vérifié l'identité et les attributs spécifiques, le cas échéant, de la personne physique concernée). Un fournisseur de services de confiance qualifié est un fournisseur de services de confiance qui fournit des services de confiance qualifiés conformément aux exigences énoncées à l'Article 3 du Règlement eIDAS. Dans la pratique, pour les signatures électroniques qualifiées, cela signifie que l'autorité de certification commerciale ou gouvernementale certifie la propriété de la clé publique d'une personne nommée en délivrant un certificat numérique.

Une signature électronique qualifiée doit également être créée par un dispositif de création de signature électronique qualifiée. Cela signifie que le logiciel ou le matériel configuré (par exemple, une carte à puce, une clé USB ou un module informatique de sécurité basé sur le cloud) est utilisé pour créer une signature qui doit satisfaire aux exigences relatives à la fiabilité des données manipulées par le dispositif telles que définies à l'Annexe II du Règlement eIDAS.

Une signature électronique qualifiée a automatiquement l'effet juridique équivalent d'une signature manuscrite et doit être reconnue comme telle dans tous les autres États membres de l'UE.

2.2 Validité et exécution des contrats électroniques

Lorsqu'on examine l'utilisation des signatures électroniques dans le contexte de contrats, l'évaluation de l'efficacité juridique de la signature électronique n'est qu'une des questions à aborder. Deux autres questions tout aussi importantes se posent. La première concerne la validité d'un accord signé électroniquement. La seconde porte sur la valeur probante et la force exécutoire d'un accord signé électroniquement.

Validité – La première question à laquelle il convient de répondre concerne les exigences formelles à remplir pour conclure valablement un contrat. Dans le droit des obligations européen, le 'consensualisme' est un principe clé. Cela signifie que le consentement libre et mutuel des parties contractantes suffit pour conclure un accord valide et qu'aucune autre exigence formelle, telle qu'un document écrit, un enregistrement ou des signatures, n'est requise.

Les contrats peuvent être conclus verbalement, par écrit, électroniquement ou même implicitement. Cependant, des exceptions à ce principe général existent dans différents États membres de l'UE. Les contrats immobiliers, les contrats de marchés publics, les contrats de consommation, les conventions de règlement, les actes de cautionnement peuvent exiger des formalités particulières à remplir afin d'être conclus valablement. Bien qu'il existe des exceptions, pour la grande majorité des contrats, le simple consentement des parties contractantes suffira et aucune signature ne sera nécessaire pour conclure un accord valide.

Exécution – La deuxième question à laquelle il faut répondre concerne la manière dont les contrats peuvent être validement exécutés. Du point de vue juridique, cette deuxième question est très pertinente puisqu'il existe une différence significative entre la conclusion d'un accord valide et la possibilité d'exécuter ledit accord en prouvant son existence et son contenu.

Les règles juridiques régissant la valeur probante et la force exécutoire des contrats varient selon la juridiction. Dans les pays de droit civil, tels que la Belgique, la France et l'Italie, qui sont regardés comme des exemples en matière de règles sur la preuve en Europe continentale ou une distinction est faite entre la preuve libre et la preuve réglementée. Dans les conflits entre professionnels (B2B), toutes les formes de preuve (par exemple, tout type d'écriture, de témoignage, de courrier électronique ou d'élément factuel) sont admissibles. Il appartient évidemment au tribunal d'évaluer la valeur probante des preuves présentées. Dans les conflits entre professionnels et consommateurs (B2C) et les conflits entre particuliers, les formes de preuve sont réglementées, c'est-à-dire que si un litige est évalué au-dessus d'un certain montant, un accord signé (un document écrit signé par les parties contractantes) est typiquement requis pour être exécuté.

Dans la plupart des juridictions, il est cependant admissible de s'écarter contractuellement des règles en matière de preuve. Cela signifie que les parties contractantes peuvent convenir des moyens de preuve qu'elles jugent suffisants et/ou de la valeur probante qui est attribuée à certains documents. Un exemple typique se trouve dans les conditions générales des services bancaires en ligne, lesquelles obligent souvent l'utilisateur à accepter que la confirmation d'une transaction avec un lecteur de carte soit considérée comme une signature électronique répondant aux exigences fonctionnelles d'une signature manuscrite.

En outre, il convient de souligner que même lorsqu'une preuve réglementée est légalement requise (comme un accord signé), les règles en matière de preuve attribueront généralement une certaine valeur probante à la preuve libre (par exemple des courriers électroniques décrivant le contenu de l'accord), suivant une règle juridique ou suivant la pratique.

Bien que des divergences existent entre les États membres de l'UE, il convient de constater (i) que la grande majorité des contrats n'exigent aucune formalité et (ii) que pour la plupart des litiges contractuels, toute preuve est admissible en vue de démontrer la force exécutoire d'un contrat.

3 EVALUATION DE LA CONFORMITÉ D'ADOBE SIGN

3.1 Description de la solution Adobe Sign

Solution Cloud – Adobe Sign est une solution de signature électronique basée sur SaaS qui permet aux utilisateurs de gérer de manière flexible le processus de signature de documents. Adobe Sign gère tous les aspects du processus de signature électronique, allant de la mise à la disposition pour ses utilisateurs d'options de validation à l'intégration de l'approbation dans le document final et en scellant ledit document avec une certification d'inviolabilité. À chaque étape du processus, Adobe Sign traite la vérification des utilisateurs en combinant tous les renseignements d'audit du signataire à sa signature dans le document. Adobe Sign peut être utilisé à l'aide du logiciel de bureau Adobe Acrobat, d'un navigateur Web, d'un appareil mobile ou via des API qui se connectent aux applications professionnelles existantes de l'utilisateur.

Processus de signature – Pour envoyer un document à signer, l'utilisateur télécharge le document sur Adobe Sign. Adobe Sign permet de faire signer électroniquement de nombreux formats de documents différents. Les utilisateurs peuvent spécifier qu'une ou plusieurs parties doivent signer le document, envoyer un message aux participants et éventuellement appliquer sur le document des contrôles de sécurité supplémentaires. Adobe Sign permet également aux utilisateurs de créer manuellement des champs de formulaire et des emplacements de signature dans un document via

une simple interface Web 'drag-and-drop'. Les signataires devront remplir les champs nécessaires et signer aux endroits appropriés lors du processus de signature.

Authentification – Adobe Sign dispose d'une série d'options pour vérifier l'identité des utilisateurs d'Adobe Sign et des signataires.

Les utilisateurs d'Adobe Sign s'authentifient eux-mêmes à l'aide d'un identifiant d'utilisateur unique créé par l'utilisateur ou attribué par un administrateur (dans le cas des comptes des entreprises). Les utilisateurs peuvent se connecter et s'authentifier grâce aux types d'identifiants d'utilisateurs suivants:

- Adobe Sign ID – Les utilisateurs utilisent une adresse e-mail et un mot de passe vérifiés pour se connecter en toute sécurité à leur compte. Les administrateurs du compte dans une organisation peuvent mettre en place des exigences supplémentaires pour le mot de passe de l'utilisateur (par exemple, une complexité minimale et un nombre de caractères minimum).
- Adobe ID – Les utilisateurs peuvent utiliser un ID Adobe pour se connecter à Adobe Sign. Un Adobe ID est un identifiant qui est utilisé par tous les services Adobe pour permettre l'accès à ces services. Les organisations ont la flexibilité de contrôler si leurs utilisateurs peuvent utiliser un Adobe ID afin de se connecter à Adobe Sign.
- Google Gmail and Google Apps – Adobe Sign permet également la connexion de l'utilisateur via un compte Google Gmail ou un compte Google Apps. Les administrateurs du compte ont la possibilité de contrôler si les utilisateurs peuvent employer cette méthode d'authentification.
- Connection unique (SSO) à l'aide du Langage SAML (Security Assertion Markup Language) – Les entreprises qui cherchent un mécanisme de contrôle d'accès plus restreint peuvent opter pour le SAML SSO qui gère de manière centralisé leurs utilisateurs à l'aide du système d'identité d'entreprise. Il permet aux administrateurs du compte d'imposer des contrôles d'accès rigoureux et de s'assurer que les exigences de mot de passe soient consistantes avec les règles internes de sécurité de l'information de l'entreprise.

En outre, Adobe Sign offre plusieurs options pour l'identification d'un signataire – lequel n'est pas nécessairement un utilisateur Adobe Sign et n'est pas tenu de s'inscrire préalablement sur Adobe Sign – qui doit être vérifiée avant que ce dernier signe un document.

L'authentification basique est obtenue en envoyant un e-mail avec un lien URL unique à un signataire. La plupart des signataires disposant d'un accès unique à un compte de messagerie électronique, cela est considéré comme le premier niveau d'authentification. Le lien URL requis pour signer le document est constitué d'identifiants uniques qui sont spécifiques à la transaction et qui peuvent être protégés par un mot de passe par l'utilisateur Adobe Sign. Après avoir cliqué sur ledit lien URL, les signataires peuvent utiliser une souris ou des styles de police prédéfinis pour créer une signature 'manuscrite' à l'écran, télécharger un fichier existant (par exemple une signature scannée) ou saisir leur nom et cliquer sur un bouton (affichant "*Cliquez pour signer*") pour signer.

En outre, Adobe Sign fournit une authentification multi-facteur et offre d'autres mécanismes d'authentification pour établir l'identité du signataire, y compris les mots de passe uniques pour les signataires individuels, une authentification téléphonique (par la voix ou par SMS) ou une identité sociale à l'aide du compte Facebook ou Google du signataire.

Certification des documents – Après que les signataires aient signé le document, Adobe Sign certifie le document afin que toute modification ultérieure soit évidente. Adobe Sign met en œuvre sa propre

PKI, qui est conforme au programme *Adobe Approved Trust List* (AATL) qui permet la certification de documents. Adobe Sign certifie automatiquement une version PDF final du document signé avant de le distribuer à tous les participants. Lorsque les destinataires téléchargent et ouvrent le fichier signé dans Adobe Acrobat ou Adobe Reader, une bannière bleue s'affiche en haut du document certifiant qu'aucune source non autorisée n'a altéré le document pendant le transit ou à aucun moment depuis l'application de la certification.

Après que tous les signataires aient signé le document, Adobe Sign enregistre aussi automatiquement tous les documents signés dans un dépôt centralisé et sécurisé où ils sont facilement accessibles, mais les utilisateurs peuvent cependant choisir d'intégrer ces services dans leurs solutions internes de gestion de documents existantes.

Piste d'audit – Adobe Sign permet une visibilité en temps réel du processus de signature. Une fois le document envoyé pour être signer, Adobe Sign utilise automatiquement le flux de travail, la surveillance, le suivi, les rappels et l'authentification pour simplifier et faciliter le processus de signature électronique.

Chaque étape clé dans le processus de signature est enregistrée, par exemple lorsque le document a été envoyé, ouvert et signé, les adresses IP ou les géolocalisations des signataires et le formulaire spécifique d'authentification utilisée pour chaque signataire ou approbateur. Le résultat est consigné dans une piste d'audit sécurisée qui fournit des preuves claires et facilement reproductibles de la signature de chaque signataire. Le rapport de suivi d'audit peut être récupéré par l'utilisateur d'Adobe Sign via le dashboard d'Adobe Sign ou par un signataire (qui n'est pas un utilisateur) en cliquant sur une signature dans le document signé et en entrant un identification de transaction unique pour accéder au rapport d'audit.

Signatures numériques – Non seulement Adobe Sign permet la création de signatures électroniques qui ne sont pas basées sur un certificat numérique, mais également permet l'utilisation de signatures numériques basées sur des certificats en utilisant Adobe Sign en combinaison avec Adobe Acrobat ou Adobe Reader afin de saisir les signatures numériques sur les documents. Pendant le processus de signature, le certificat du signataire est cryptographiquement joint au document en utilisant la clé privée détenue par ce signataire. Au cours du processus de validation, la clé publique réciproque est extraite de la signature et est utilisée pour à la fois authentifier l'identité du signataire et garantir qu'aucune modification n'a été apportée au document depuis qu'il a été signé. À cet égard, la piste d'audit fournit également des informations supplémentaires précieuses telles que l'adresse IP ou la géolocalisation du signataire.

Adobe n'est pas une autorité de certification. Par conséquent, Adobe Sign ne délivre pas lui-même des certificats numériques mais fonctionne avec pratiquement tous les certificats numériques émis par des prestataires de services de confiance, dont de nombreux sont reconnus par Adobe Sign via *l'Adobe Approved Trust List* (ex. cette liste inclut les prestataires de services de confiance tels que DigiCert, GlobalSign, QuoVadis, etc.).

Sécurité du Cloud – Adobe a mis en place un certain nombre de mesures techniques et organisationnelles liées à la sécurité des centres de données, aux plans de reprise d'activités, aux contrôles environnementaux, à la sécurité logique, à la protection des données, à la détection des intrusions, aux plans de réponse et à la surveillance afin de garantir la sécurité d'Adobe Sign ainsi que

de tous les processus associés. Les processus professionnels d'Adobe Sign sont certifiés conformes aux normes ISO 270001, SSAE SOC 2 Type 2 et PCI DSS.

Plans d'abonnement – Adobe Sign peut être utilisé avec trois plans d'abonnements différents: 'individuel', 'professionnel' et 'entreprise'. Selon le plan d'abonnement choisi, Adobe Sign offre des fonctionnalités supplémentaires. En particulier, l'authentification multi-facteurs n'est disponible qu'avec les plans d'abonnement 'professionnel' et 'entreprise', alors que l'utilisation de signatures électroniques basées sur un certificat numérique n'est disponible qu'avec le plan d'abonnement 'entreprise'.

3.2 Comment Adobe Sign peut assurer une conformité au Règlement eIDAS

Cette section du document examine comment les exigences légales pour les signatures électroniques standards, avancées et qualifiées telles que définies dans les sections précédentes s'appliquent à Adobe Sign.

3.2.1 Adobe Sign se conforme aux exigences européennes relatives aux signatures électroniques standards

Exigences – Conformément à la définition de "signatures électroniques" standards dans le Règlement eIDAS, les données sous forme électronique doivent être jointes ou logiquement associées à d'autres données sous une forme électronique et doivent être utilisées par le signataire lorsque ce dernier signe.

Adobe Sign – En ce qui concerne la description de la solution d'Adobe Sign telle que décrite ci-dessus, nous concluons avec certitude que, d'un point de vue juridique, Adobe Sign se conforme ou même dépasse les exigences légales relatives aux signatures électroniques standards:

- '*données sous forme électronique*' – Les signatures électroniques créées avec Adobe Sign consistent en effet en une série de données sous forme électronique.
- '*jointes ou associées logiquement à d'autres données sous forme électronique*' – La signature électronique peut être jointe par le signataire à une variété de documents électroniques, puisque Adobe Sign permet le téléchargement de plusieurs formats différents de documents.
- '*que le signataire utilise pour signer*' – Adobe Sign a été conçu d'une telle manière que l'intention du signataire de signer est clairement capturée dans le processus de la signature:
  - Le signataire recevra un e-mail intitulé "*Veuillez signer* [Nom du document]*"* dans lequel un lien hypertexte vers Adobe Sign indique ce qui suit: "*Cliquez ici pour revoir et signer* [Nom du document]*"*;
  - Lorsque le signataire revoit le document, il est prié de signer le document en tapant son nom, en créant une signature 'manuscrite' sur l'écran ou en téléchargeant une image d'une signature scannée. Le signataire est invité à le faire par le biais d'un formulaire dans le document qui mentionne "*Cliquez ici pour signer*".
  - Après cette étape, une notification apparaît indiquant que "*J'accepte les Conditions d'Utilisation et les Demandes de Divulgation des Consommateurs de ce document*" avec un

bouton "*Cliquer pour signer*". Lorsque le signataire clique sur ce bouton et confirme une deuxième fois son intention de signer le document, Adobe Sign considère que le document a été signé et communique le document aux autres participants.

Bien que l'apparence de la signature sur le document ne puisse être vue que comme une caractéristique visuelle et esthétique sans influencer d'aucune manière la valeur de la signature électronique, la multi-approche en vue de capturer l'intention du signataire de signer le document permet de répondre au troisième critère. Il ne s'agit pas seulement d'une obligation de produire des signatures électroniques standards, mais aussi d'un aspect important au niveau de la formation du contrat. Les contrats sont, en principe, conclus par le biais du consentement mutuel des parties contractantes, le fait dès lors d'avoir un processus de signature clair contribue à démontrer la volonté du signataire d'être lié par des obligations légales et d'en déduire son consentement.

Cela signifie, selon l'Article 25.1 du Règlement eIDAS, qu'une signature électronique produite avec Adobe Sign ne peut, en principe, se voir refuser un effet juridique et la recevabilité pour valoir comme preuve dans le cadre de procédures judiciaires pour des raisons uniquement techniques. Cela ne signifie toutefois pas qu'une telle signature électronique acquiert automatiquement la même valeur juridique qu'une signature manuscrite, à moins évidemment qu'un certificat qualifié soit utilisé (voir la section 3.2.3 ci-dessous).

En outre, Adobe Sign offre un certain nombre de fonctionnalités qui pourraient renforcer le caractère exécutoire comme une signature électronique, par rapport à d'autres signatures électroniques couramment acceptées, telles que:

- La piste d'audit – Si la validité de la signature électronique est contestée, la piste d'audit générée par Adobe Sign pourrait servir de preuve pertinente pour démontrer le lien entre l'identité d'un signataire et d'une signature.
- Les méthodes d'authentification multi-facteurs – Si l'authentification multi-facteurs était requise par le signataire, en sélectionnant les paramètres appropriés, cela accroîtra inévitablement la capacité d'authentifier correctement le signataire et de produire des signatures électroniques avec une valeur probante beaucoup plus accrue.

Il s'ensuit qu'Adobe Sign n'est pas simplement une solution qui permet de produire des signatures électroniques standards en conformité avec le Règlement eIDAS mais il peut également être considéré qu'Adobe Sign est un moyen sûr et fiable de le faire.

Adobe Sign permet de produire des signatures électroniques standards de manière fiable et sécurisée. Adobe Sign (i) permet d'identifier les signataires d'une manière avancée, (ii) de capturer l'intention des signataires de signer un document de manière non ambiguë et (iii) de gérer un enregistrement de piste d'audit afin de renforcer le caractère exécutoire de la signature électronique produite.

3.2.2 Adobe Sign et les signatures électroniques avancées

Exigences – Conformément à la définition de signatures électroniques avancées dans le Règlement eIDAS, une telle signature électronique doit être liée au signataire de manière univoque, permettre d'identifier le signataire, avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif et être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Adobe Sign – En ce qui concerne la description de la solution Adobe Sign telle qu'indiquée ci-dessus, nous concluons avec certitude que, d'un point de vue juridique, Adobe Sign permet la production de signatures électroniques avancées basées sur des certificats numériques.

Comme il est indiqué ci-dessus, les exigences relatives aux signatures électroniques avancées sont généralement remplies par des signatures électroniques fondées sur des certificats numériques et nous avons noté qu'Adobe n'émet pas et ne gère pas de tels certificats pour produire ces signatures. Adobe Sign contient, cependant, une intégration initiale avec Adobe Acrobat et Adobe Reader qui permet la création de telles 'signatures numériques'. Afin de dissiper tout doute, il convient de souligner que le concept de 'signature numérique', tel qu'utilisé par Adobe Sign, n'est pas défini légalement dans le Règlement eIDAS, mais doit être interprété comme incluant les signatures numériques basées sur des certificats ainsi que les signatures électroniques fondées sur des certificats auto-signés.

Si un document est téléchargé dans Adobe Sign pour être signé, l'utilisateur Adobe Sign peut exiger que les signataires utilisent une signature numérique en ajoutant un champ de formulaire pour la signature numérique au document. Les signataires seront alors invités à télécharger le document, qui s'ouvrira dans Adobe Acrobat ou Adobe Reader (en fonction de ce qui est installé sur l'ordinateur du signataire). Ensuite le signataire sera guidé vers le champ de formulaire relatif à la signature et sera en mesure de sélectionner un certificat dans son dispositif et d'appliquer la signature électronique avancée au document dans Adobe Acrobat ou Adobe Reader. Le document signé sera alors automatiquement téléchargé sur Adobe Sign (sans que d'autres actions spécifiques ne soient requises), les autres signataires seront notifiés et un enregistrement de la signature numérique sera saisi dans la piste d'audit pour le document. Bien que la piste d'audit mentionne uniquement que le document a été signé numériquement, la validité du certificat numérique qui a été utilisé, peut être vérifiée par l'utilisateur d'Adobe Sign ainsi que les autres signataires en consultant le document signé via Adobe Sign ou en ouvrant le document directement dans Adobe Reader ou Adobe Acrobat.

Les signatures électroniques avancées basées sur les certificats numériques peuvent être intégrées dans tout un processus de signature électronique qui est totalement pris en charge et géré par Adobe Sign.

Comme indiqué dans la section 2.1.2 ci-dessus, il existe des arguments pour affirmer que les technologies relatives aux signatures autres que la cryptographie à clé publique, comme par exemple les solutions de signature électronique basées sur un processus lié au cloud, peuvent satisfaire aux

exigences des signatures électroniques avancées. Par conséquent, si la fonctionnalité 'signatures numériques' d'Adobe Sign n'est pas prise en compte et que la solution est évaluée en fonction des quatre critères d'une signature électronique avancée, les points suivants doivent être observés:

- *'être liée au signataire de manière univoque'* – Adobe Sign permet de lier toutes les signatures électroniques produites sur la plate-forme à un signataire. Adobe Sign propose des méthodes d'authentification multi-facteurs afin d'authentifier clairement les signataires. En outre, la piste d'audit permet de suivre toutes les signatures électroniques dans un document qui peut lier une signature spécifique à un signataire spécifique.
- '*permettre d'identifier le signataire*' – Afin de s'assurer que cette exigence est satisfaite, les utilisateurs sont invités à exiger l'authentification multi-facteurs pour s'identifier et signer le document, au lieu de simplement exiger de cliquer sur un lien hypertexte afin d'accéder au document.
- *'avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif'* – En règle générale, seules les signatures électroniques avancées basées sur des certificats numériques sont considérées comme pouvant répondre à ce critère. Selon ce dernier, la clé privé utilisée par le signataire est considérée comme la 'donnée de création de signature électronique'. Le concept de 'données de création de signature électronique' n'est cependant pas nécessairement limité aux clés privées puisque le Règlement eIDAS le définit de manière large comme 'des données uniques utilisées par le signataire pour créer une signature électronique'.

En ce qui concerne le Considérant 52 du Règlement eIDAS, les solutions de signature électronique basées sur le cloud (qui ne sont pas nécessairement basées sur des certificats numériques) peuvent satisfaire à ce critère à condition que des procédures spécifiques en termes de gestion et de sécurité soient mises en place et que des systèmes et produits fiables soient utilisés afin de garantir que l'environnement qui entoure la création de la signature électronique est fiable et sous le seul contrôle du signataire. Lorsque des méthodes d'authentification multi-facteurs rigoureuses sont utilisées pour accéder à l'environnement personnalité de la signature et au document à signer en lui-même, il peut être soutenu que la plate-forme d'Adobe Sign permet effectivement de créer des signatures électroniques avec des moyens de haut niveau de confiance sous le contrôle du signataire. À cet égard, il faut souligner que les administrateurs Adobe eux-mêmes n'ont accès à aucun compte d'utilisateur ni à aucun profil des signataires, ni à aucun détail relatif à l'identification des utilisateurs (y compris les mots de passe) pour accéder à leur compte ou profil.

- *'être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable'* – Après que les signataires aient signé le document, Adobe Sign certifie automatiquement le document signé avec son certificat numérique en vue de protéger le document contre tout changement ultérieur. De plus, lorsqu'un document est signé avec Adobe Sign, tout changement ultérieur devient facilement visible puisque la piste d'audit enregistre toutes les activités et les modifications ultérieures du document concerné.

Bien que des arguments existent pour affirmer qu'Adobe Sign permet de produire des signatures électroniques avancées qui ne sont pas basées sur un certificat numérique, il faut souligner que ces arguments n'ont pas encore été présentés devant un tribunal. Néanmoins, les utilisateurs d'Adobe Sign doivent toujours garder à l'esprit que le Règlement eIDAS ne confère pas à la signature électronique avancée des effets juridiques spécifiques différents d'une signature électronique

standard. Par conséquent, même si un tribunal décide qu'Adobe Sign, sans utiliser de certificats numériques, ne permet pas de produire des signatures électroniques avancées, cela ne signifie pas que la fiabilité et la sureté d'Adobe Sign diminueraient. En tout état de cause, tel qu'indiqué ci-dessus, Adobe Sign doit être considéré comme un outil sûr et fiable pour les processus de signature électronique.

Des arguments valables existent pour affirmer qu'Adobe Sign permet de produire des signatures électroniques avancées qui ne sont pas basées sur un certificat numérique.

3.2.3 Adobe Sign et les signatures électroniques qualifiées

Exigences – Conformément au Règlement eIDAS, une signature électronique qualifiée est juridiquement équivalente à une signature manuscrite et doit être reconnue comme telle dans tous les autres États membres de l'UE. Tel qu'indiqué ci-dessus, le Règlement eIDAS définit une signature électronique qualifiée comme une signature électronique avancée avec les exigences supplémentaires qu'elle doit reposer sur un certificat qualifié de signature électronique et être créée à l'aide d'un dispositif de création de signature électronique qualifiée.

La première exigence est l'utilisation d'un certificat qualifié. Il s'agit d'un certificat numérique émis par un prestataire de service de confiance qui satisfait aux exigences de l'Annexe I du Règlement eIDAS. En ce qui concerne les exigences du Règlement eIDAS, un certificat contenant une clé de signataire et l'identité du propriétaire délivrée par une autorité de certification commerciale ou gouvernementale qualifiée est conforme à la définition d'un certificat qualifié.

La deuxième exigence est l'utilisation d'un dispositif de création de signature électronique qualifiée. Un tel dispositif est configuré sur du matériel informatique ou sur un logiciel informatique (par exemple une carte à puce, une clé USB ou un module informatique de sécurité basé sur le cloud), est utilisé pour créer une signature électronique et satisfait aux exigences de l'Annexe II du Règlement eIDAS.

Adobe Sign – Adobe Sign ne gère, ni ne délivre de certificats qualifiés et n'offre pas d'outils de création de signature électronique qualifiée, mais nous concluons toutefois avec certitude que, d'un point de vue juridique, Adobe Sign permet de soutenir la production de signatures électroniques qualifiées par le biais de son interopérabilité avec des fournisseurs de certificats qualifiés.

Adobe Sign contient une intégration d'origine avec Adobe Acrobat et Adobe Reader pour permettre des 'signatures numériques'. Afin de dissiper tout doute, il convient de souligner que le concept de 'signature numérique' utilisé par Adobe Sign n'est pas légalement défini dans le Règlement eIDAS, mais doit être interprété comme incluant les signatures électroniques avancées basées sur des certificats numériques, des signatures électroniques qualifiées ainsi que des signatures électroniques basées sur des certificats auto-signés.

Si un document est téléchargé dans Adobe Sign pour être signé, l'utilisateur Adobe Sign peut exiger que les signataires utilisent une signature numérique en ajoutant un champ de formulaire pour la signature numérique au document. Les signataires seront alors invités à télécharger le document, qui s'ouvrira dans Adobe Acrobat ou Adobe Reader (en fonction de ce qui est installé sur l'ordinateur du signataire), ensuite le signataire sera guidé vers le champ de formulaire relatif à la signature et sera en mesure de sélectionner un certificat dans son dispositif et d'appliquer la signature électronique avancée au document dans Adobe Acrobat ou Adobe Reader. Le document signé sera alors automatiquement téléchargé sur Adobe Sign (sans que d'autres actions spécifiques ne soient requises), les autres signataires seront notifiés et un enregistrement de la signature numérique sera saisi dans la piste d'audit pour le document. Bien que la piste d'audit mentionne uniquement que le document a été signé numériquement, la validité du certificat numérique qui a été utilisé, peut être vérifiée par l'utilisateur d'Adobe Sign ainsi que les autres signataires en consultant le document signé via Adobe Sign ou en ouvrant le document directement dans Adobe Reader ou Adobe Acrobat.

Dans certains cas, l'utilisation de signatures électroniques qualifiées est requise afin de signer valablement un contrat électronique, il est recommandé aux utilisateurs et signataires d'Adobe Sign de vérifier que les paramètres appropriés sont activés afin de pouvoir conclure un contrat valide.

Par souci d'exhaustivité, il faut mentionner qu'Adobe Acrobat et Adobe Reader possèdent des fonctionnalités permettant d'identifier des certificats qualifiés, par le biais de déclarations de certificat qualifié standard et sur la base de la Liste de l'EU pour les prestataires de services de confiance; de valider et d'accepter des certificats qualifiés basés sur la UE; d'identifier les dispositifs de création de signature qualifiée au moyen de déclarations de certificat qualifié standard; et de supporter les signatures numériques dans le format PAdES Baseline (le ETSI TS 103 172 ainsi que le récent ETSI EN 319 142-1).

Les signatures électroniques qualifiées peuvent être intégrées dans tout un processus de signature électronique qui est totalement pris en charge et géré par Adobe Sign.

4 CONCLUSION

Adobe Sign est une solution de signature électronique basée sur SaaS qui gère tous les aspects du processus de signature électronique, allant de la mise à la disposition pour ses utilisateurs d'options de validation à l'intégration de l'approbation dans le document final et en scellant ledit document avec une certification d'inviolabilité.

Adobe Sign prend en charge une série d'options pour vérifier l'identité des utilisateurs et des signataires d'Adobe Sign, en utilisant notamment des identifiants spécifiques (par exemple, l'identifiant Adobe Sign ou le compte Google Gmail) et des méthodes d'authentification (multi-facteurs) (par exemple des mots de passe uniques, une authentification téléphonique (par la voix ou par sms) ou

l'identité sociale). En outre, les processus sous-jacents à Adobe Sign ont été créés d'une telle manière qu'ils saisissent l'intention des signataires. Enfin, pour protéger le document signé contre toute modification ultérieure, Adobe Sign maintient une piste d'audit qui enregistre les modifications apportées au document signé et certifie le document final avant de le communiquer aux autres participants.

D'un point de vue juridique, nous pouvons conclure avec certitude que lorsque les paramètres d'utilisateur appropriés sont sélectionnés, Adobe Sign est un outil fiable et sécurisé qui permet de produire des signatures électroniques standards qui se conforment ou même dépassent les exigences d'une "signature électronique" telle que définie à l'Article 3.10 du Règlement eIDAS. Cela signifie que, conformément à l'Article 25.2 du Règlement eIDAS, leur effet juridique ne peut leur être refusé sur la base de leurs caractéristiques uniquement techniques. Bien qu'une signature électronique standard n'ait pas automatiquement le même effet juridique qu'une signature manuscrite, du point de vue de l'utilisation prévue des signatures électroniques, comme moyen pour conclure plus facilement et librement des contrats valides, ainsi qu''au niveau de la force exécutoire, la signature électronique standard est souvent considérée comme adéquate.

Lorsque les tribunaux doivent évaluer la force probante des preuves qui leur sont présentées, ils donneront généralement plus de valeur aux documents qui sont signés électroniquement à l'aide d'une technologie fiable et sécurisée. À cet égard, Adobe Sign fournit une valeur probante importante en fournissant une authentification multi-facteurs, en enregistrant chaque action sur Adobe Sign et en certifiant le document signé.

En outre, nous pensons qu'il existe des arguments pour affirmer qu'Adobe Sign, sans l'utilisation de la technologie de signature numérique, permet de produire des 'signatures électroniques avancées' au sens de l'Article 3.11, du Règlement eIDAS. Étant donné que le Règlement eIDAS n'attribue pas d'effets juridiques spécifiques aux signatures électroniques avancées autres que les signatures électroniques standards, il convient de souligner que même si les exigences légales d'une signature électronique avancée ne sont pas remplies, Adobe Sign doit continuer à être considéré comme une solution de signature électronique fiable et sécurisée. Par ailleurs, Adobe Sign contient également une option qui supporte l'utilisation de la technologie de signature numérique, notamment les signatures électroniques avancées basées sur des certificats numériques et les "signatures électroniques qualifiées" au sens de l'Article 3.12 du Règlement eIDAS. Par conséquent, si cette option est activée par l'utilisateur, Adobe Sign peut être considéré comme un outil facile d'utilisation pour les entreprises en vue de supporter et de faciliter le processus de production de signatures électroniques avancées et qualifiées. Dans le cas de signatures électroniques qualifiées, Adobe Sign permet la création de signatures électroniques qui, conformément à l'Article 25 du Règlement eIDAS, ont un effet juridique équivalent à une signature manuscrite et sont reconnues dans tous les autres États membres de l'UE.

Adobe Sign est une solution de signature électronique fiable qui permet de gérer un processus de signature conforme à tous les types de signatures électroniques disponibles sous le Règlement eIDAS. Adobe Sign permet en particulier aux utilisateurs de configurer et de définir des flux de travail selon leur conformité particulière, de l'industrie et des risques.

5 SUR L'AUTEUR

Prof. Dr. Patrick Van Eecke est un associé du département du droit des technologies de l'information de DLA Piper à Bruxelles. Patrick est membre du barreau de Bruxelles et membre associé de l'association du barreau américain. Le Dr. Van Eecke conseille les administrations publiques ainsi que les entreprises sur la conformité des solutions de signature électronique et a acquis une grande expérience dans la rédaction et la négociation de documents juridiques liés aux PKI, tels que les *Certification Practices Statements*, *Certificate Policies*, *Signatures Policies* et *Relying Party Agreements*.

Patrick Van Eecke est impliqué dans divers projets de recherche et de consultation pour la Commission Européenne et plusieurs gouvernements nationaux. Par exemple, il a été impliqué dans la première étude de la Commission Européenne sur les aspects juridiques des signatures électroniques (1998), l'étude de la Commission Européenne sur les politiques de signature électronique (2001), l'étude de la Commission Européenne sur l'archivage à long terme des signatures électroniques (2001) et l'étude de la Commission Européenne sur les aspects juridiques et commerciaux des signatures électroniques (2003). Il a été consultant principal dans l'étude de la Commission Européenne sur l'avenir de la politique de normalisation des TIC (2006). Plus récemment, il a été impliqué dans l'étude de la Commission européenne sur la politique d'identification, d'authentification et de signature (IAS) (2010) ainsi que dans l'étude relative aux prestataires de services de confiance pour les transactions électroniques dans le marché intérieur (2014).

En tant que représentant national, Patrick a participé aux débats du Conseil Européen sur la directive relative aux signatures électroniques et sur la directive relative au commerce électronique. Il conseille également le Comité Economique et Social des Communautés Européennes sur ces questions. En tant qu'expert juridique de l'équipe d'experts de l'EESSI, (European Electronic Signature Standardisation Initiative) il a été co-auteur du premier rapport EESSI et suit les réalisations légales y relatives.

Dr. Van Eecke a obtenu son doctorat à l'Université de Leuven (y compris une bourse d'études à l'Université de Stanford aux Etats-Unis) ayant comme sujet "Le statut légal des signatures électroniques" (2003). Il est professeur à l'Université d'Anvers ou il enseigne le droit européen de l'information et des communications. Il est également invité comme intervenant à Kings College et à l'Université de Queen Mary (Londres). Patrick est l'auteur de plusieurs articles juridiques et de livres sur la criminalité informatique, les signatures électroniques, les contrats électroniques et la vie privée. Il est également régulièrement orateur à des conférences nationales et internationales.

* *

*

www.dlapiper.com