Adobe Sign

Die Einhaltung der für elektronische Signaturen geltenden europäischen Gesetze

März 2017

DLA PIPER

Adobe

INHALTSVERZEICHNIS

1 Einführung

Dieses Dokument befasst sich mit der rechtlichen Wirksamkeit der Lösung Adobe Sign in Bezug auf die in Europa geltenden Anforderungen an elektronische Signaturen. Im ersten Teil geben wir Ihnen einen Überblick über das maßgebliche gesetzliche Rahmenwerk und beschreiben kurz den Umfang, die wesentlichen Konzepte und die rechtlichen Konsequenzen der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (im Folgenden als „eIDAS-Verordnung“ beziehungsweise „Verordnung“ bezeichnet). Dabei handelt es sich um das Schlüsseldokument, das die Wirksamkeit elektronischer Signaturen in der EU regelt. Wir werden zudem wichtige Fragen zur Wirksamkeit und Durchsetzbarkeit elektronisch unterzeichneter Vereinbarungen erörtern.

Im zweiten Teil dieses Dokuments geht es um die Kernmerkmale von Adobe Sign. Wir prüfen diese Kernmerkmale im Hinblick auf die relevanten gesetzlichen Anforderungen, mit dem Ziel, die Rechtsverbindlichkeit einer mithilfe von Adobe Sign erstellten elektronischen Signatur zu analysieren.

Unser Fazit: Adobe Sign ist bei Auswahl der richtigen Benutzereinstellungen aus rechtlicher Sicht ein vertrauenswürdiges und sicheres Tool, das es ermöglicht, elektronische Signaturen zu erstellen, die den in Artikel 3 (10) der eIDAS-Verordnung formulierten Anforderungen entsprechen oder sogar darüber hinausgehen.

Darüber hinaus spricht unserer Ansicht nach vieles dafür, dass Adobe Sign es ermöglichen könnte, fortgeschrittene elektronische Signaturen, wie in Artikel 3 (11) der eIDAS-Verordnung definiert, ohne die Verwendung von Technologien für digitale Signaturen zu erstellen.

Zudem können wir beobachten, dass Adobe Sign auch eine Option bietet, welche die Verwendung digitaler Signaturtechnologien unterstützt, insbesondere für digitale, zertifikatsbasierte, fortgeschrittene elektronische Signaturen sowie für qualifizierte elektronische Signaturen, wie in Artikel 3 (12) der eIDAS-Verordnung definiert. Bei Aktivierung der entsprechenden Option durch den Nutzer kann Adobe Sign als ein unternehmensfreundliches Tool bezeichnet werden, das die Erstellung fortgeschrittener und qualifizierter elektronischer Signaturen unterstützt und erleichtert.

In Anbetracht der vorstehenden Überlegungen kann Adobe Sign bei entsprechender Konfiguration als eine zuverlässige Lösung für elektronische Signaturen betrachtet werden, die es dem Nutzer erlaubt, den gesamten Unterzeichnungsprozess in einer Weise abzuwickeln, die mit sämtlichen Arten von elektronischen Signaturen, welche die eIDAS-Verordnung vorsieht, kompatibel ist. Adobe Sign erlaubt es dem Nutzer, Workflows entsprechend seinem individuellen Compliance-, Branchen- und Risikoprofil zu konfigurieren und aufzubauen.

2 Regulatorische Rahmenbedingungen

2.1 Die eIDAS-Verordnung

Die eSign-Richtlinie – Bis vor wenigen Monaten richtete sich die Verwendung elektronischer Signaturen in der EU nach der Richtlinie 1999/93/EG, die für die Gemeinschaft einen Rahmen für elektronische Signaturen schuf (eSign-Richtlinie). Die Harmonisierung, die mit dieser Richtlinie erreicht wurde, erwies sich jedoch als unzureichend. Dies führte zu einer fehlenden Interoperabilität der verschiedenen elektronischen Signaturlösungen der einzelnen EU-Mitgliedsstaaten untereinander und in der Folge zu einer Marktfragmentierung. Wenngleich die Richtlinie die Rechtswirkungen elektronischer Signaturen im Einzelnen regelte, stellte sie nicht sicher, dass die Anerkennung einer elektronischen Signatur in einem EU-Mitgliedstaat auch die Anerkennung derselben elektronischen Signatur in einem anderen EU-Mitgliedsstaat implizierte. Somit war die Akzeptanz elektronischer Signaturen bei grenzüberschreitenden elektronischen Transaktionen höchst fragwürdig. Darüber hinaus eignete sich die Richtlinie nicht für innovative Lösungen, welche die Möglichkeit bieten, anzuzeigen, dass eine Person den Inhalt eines elektronischen Dokuments oder einer elektronischen Vereinbarung akzeptiert hat.

Um die Verwendung elektronischer Signaturen und anderer Vertrauensdienste voranzutreiben und einen Beitrag zur Schaffung eines einheitlichen digitalen Marktes für die gesamte EU zu leisten, verabschiedete der europäische Gesetzgeber im Juli 2014 die eIDAS-Verordnung. Die eIDAS-Verordnung, deren Bestimmungen zum größten Teil erst seit dem 1. Juli 2016 Anwendung finden, trat an die Stelle der vorgenannten Richtlinie für elektronische Signaturen. Sie baut auf den in dieser Richtlinie bereits niedergelegten Prinzipien auf, die sie dabei konkretisiert und zugleich erweitert.

Die eIDAS-Verordnung – Da der europäische Gesetzgeber sich entschied, eine Verordnung zu erlassen (die unmittelbar in allen EU-Mitgliedstaaten gilt), anstatt die Richtlinie zu überarbeiten (die in den einzelnen Mitgliedsstaaten erst in nationales Recht hätte umgesetzt werden müssen), müssen die Unternehmen sich nunmehr nicht länger mit den nationalen Gesetzen für elektronische Signaturen auseinandersetzen. Sie brauchen nur noch ein einheitliches Regelwerk zu beachten, wodurch sich das Risiko von Auslegungsstreitigkeiten erheblich verringert. Wenngleich die eIDAS-Verordnung darauf abzielt, die rechtliche Wirksamkeit von elektronischen Signaturen und deren Zulassung als Beweismittel in Gerichtsverfahren sicherzustellen, regelt sie ebenso wenig wie ihre Vorgängerin konkret den Abschluss und die Wirksamkeit von (elektronischen) Vereinbarungen (siehe unten Ziffer 2.2).

Die eIDAS-Verordnung unterscheidet zwischen einfachen elektronischen Signaturen, fortgeschrittenen elektronischen Signaturen und qualifizierten elektronischen Signaturen.

2.2 Einfache elektronische Signaturen

Weitgefasste Definition – Die eIDAS-Verordnung enthält eine weitgefasste Definition der einfachen elektronischen Signatur und verweist dabei auf keine spezielle Technologie. Diese „einfache elektronische Signatur“ bezeichnet Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet.

In Erwägungsgrund 26 der eIDAS-Verordnung wird angesichts des Tempos des technologischen Wandels ein für Innovationen offener Ansatz propagiert. Außerdem wird in Erwägungsgrund 27 betont, dass die Verordnung technologieneutral sein sollte und dass die von ihr ausgehenden Rechtswirkungen mit allen technischen Mitteln erreichbar sein sollten (sofern dadurch die Anforderungen der Verordnung jeweils erfüllt

werden). Folgende drei Kriterien müssen für eine einfache elektronische Signatur erfüllt sein: (i) das Vorliegen von Daten in elektronischer Form, (ii) die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden sind und (iii) die der Unterzeichner zum Unterzeichnen verwendet. Diese Kriterien werden in der eIDAS-Verordnung nicht näher definiert oder erklärt. Somit bleibt sowohl Auslegungsspielraum als auch Raum für technologische Innovationen. In der Praxis bedeutet dies, dass viele elektronische Tools, welche die Absicht des Unterzeichners erfassen, den Inhalt eines Dokuments anzuerkennen, als elektronische Signatur betrachtet werden können. Das können unter anderem ein PIN-Code, ein Passwort, eine eingescannte Unterschrift, eine symmetrische oder eine auf öffentlichen Schlüsseln basierende Kryptografie für Signaturen oder eine biometrische Signatur sein.

Rechtswirkung – Gemäß Artikel 25.1 der eIDAS-Verordnung dürfen einer einfachen elektronischen Signatur die Rechtswirkung und die Zulassung als Beweismittel in Gerichtsverfahren nicht allein aus dem Grund versagt werden, dass sie in elektronischer Form vorliegt oder dass sie nicht den Anforderungen an qualifizierte elektronische Signaturen entspricht. Wenngleich es den EU-Mitgliedstaaten weiterhin freisteht, die Rechtswirkungen einfacher elektronischer Signaturen zu definieren, bewirkt Artikel 25.1 doch, dass es diesen Staaten verwehrt ist, Gesetze zu erlassen oder beizubehalten beziehungsweise nationale Regelungen zu bestätigen oder zu genehmigen, denen zufolge die Verwendung von elektronischen Signaturen alleine aus dem Grund abgelehnt wird, dass solche Signaturen in elektronischer Form vorliegen oder nicht qualifiziert sind.

Die Tatsache, dass einer einfachen elektronischen Signatur die Rechtswirkung und die Zulassung als Beweismittel nicht aufgrund bestimmter technischer Merkmale versagt werden dürfen, bedeutet jedoch nicht, dass eine solche Signatur rechtlich genauso zu behandeln ist wie eine handschriftliche Unterschrift. Das ist nur der Fall, wenn die entsprechenden Gesetze dies ausdrücklich so vorsehen. Ebenso wenig sind nationalstaatliche Regelungen bezüglich der freien Beweiswürdigung durch die Gerichte davon betroffen.

> Einer einfachen elektronischen Signatur dürfen die Rechtswirkung und die Zulassung als Beweismittel in Gerichtsverfahren nicht alleine aus dem Grund versagt werden, dass sie in elektronischer Form vorliegt oder dass sie nicht den Anforderungen an qualifizierte elektronische Signaturen entspricht.

2.3 Fortgeschrittene elektronische Signaturen

Vier Kriterien – Eine „fortgeschrittene elektronische Signatur“ definiert Artikel 3 (10) der eIDAS-Verordnung als eine einfache Signatur, die den Anforderungen des Artikel 26 der eIDAS-Verordnung genügt, nämlich: (a) sie ist eindeutig dem Unterzeichner zugeordnet, (b) sie ermöglicht die Identifizierung des Unterzeichners, (c) sie wird unter Verwendung von elektronischen Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann und (d) sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Wenngleich die rechtliche Definition der fortgeschrittenen elektronischen Signatur in einer technologieneutralen Art und Weise formuliert wurde, wird diese Definition nach der bis heute allgemein anerkannten Meinung so ausgelegt, dass sich das bezeichnete Konzept auf elektronische Signaturen bezieht, die auf einer digitalen Signaturtechnologie beruhen oder – mit anderen Worten – die sich auf öffentlichen Schlüsseln basierender Kryptografie bedienen. Entsprechend dieser Auslegung ist unter einer fortgeschrittenen elektronischen Signatur eine digitale Datei zu verstehen, die einen durch Verschlüsselung mit einem privaten Schlüssel des Unterzeichners erzeugten Hash-Code des Dokuments enthält. Folglich kann die fortgeschrittene elektronische Signatur mit dem entsprechenden öffentlichen Schlüssel des Unterzeichners verifiziert werden. Ein entsprechendes digitales Zertifikat, insbesondere in Form einer digitalen Bescheinigung, welche die Daten zum

Zweck der Validierung der Unterschrift mit einer natürlichen Person in Verbindung bringt und das zumindest den Namen beziehungsweise das Pseudonym der betreffenden Person bestätigt, weist den Unterzeichner als Inhaber des öffentlichen Schlüssels aus.

Fernsignaturen – Die technologieneutrale Definition der fortgeschrittenen elektronischen Signatur schließt jedoch nicht aus, dass auch andere Technologien die Erstellung einer fortgeschrittenen elektronischen Signatur ermöglichen können. Dies setzt voraus, dass die oben bezeichneten vier Kriterien jeweils erfüllt werden. Einerseits wird in den Erwägungsgründen 26 und 27 versichert, dass die eIDAS-Verordnung einen für Innovationen offenen Ansatz propagiert und dass die von ihr ausgehenden Rechtswirkungen mit allen technischen Mitteln erreicht werden können. Andererseits bereitet Erwägungsgrund 52 auch den Weg für die rechtswirksame Verwendung von Cloud-basierten elektronischen Signaturlösungen. Entsprechend diesem Erwägungsgrund wird anerkannt, dass Cloud-basierte elektronische Signaturlösungen in einer von einem Vertrauensdiensteanbieter im Namen des Unterzeichners geführten Umgebung ausgebaut werden sollten. Darüber hinaus wird diesbezüglich klargestellt, dass solche elektronischen Signaturen tatsächlich rechtlich in gleicher Weise anerkannt werden sollen wie elektronische Signaturen, die vollständig in der Umgebung des Nutzers erstellt werden. Dies setzt voraus, dass die Anbieter von elektronischen Fernsignaturdiensten spezielle Verfahren für das Management und die administrative Sicherheit einrichten und mit vertrauenswürdigen Systemen und Produkten arbeiten, um auf diese Weise für eine vertrauenswürdige Umgebung für die Erstellung elektronischer Signaturen zu sorgen und zu gewährleisten, dass eine solche Umgebung unter der alleinigen Kontrolle des Unterzeichners genutzt werden kann. Angesichts der weitgefassten Formulierung dieses Erwägungsgrunds kann man argumentieren, dass der Unterzeichner seinen privaten Schlüssel in der Cloud speichern oder sogar eine Cloud-basierte elektronische Signaturlösung verwenden darf, für die keine Unterzeichnerschlüssel erforderlich sind.

Die eIDAS-Verordnung verleiht der fortgeschrittenen elektronischen Signatur keine konkreten Rechtswirkungen, die sich von den Rechtswirkungen einfacher elektronischer Signaturen unterscheiden würden. Das Konzept dient jedoch als Baustein für die Definition der qualifizierten elektronischen Signatur, worunter eine fortgeschrittene elektronische Signatur zu verstehen ist, die eine Reihe von zusätzlichen rechtlichen Anforderungen erfüllt (siehe unten Ziffer 2.1.3).

Erhöhtes Maß an Vertrauen – Der Hauptunterschied zwischen einfachen elektronischen Signaturen und fortgeschrittenen elektronischen Signaturen besteht darin, dass die technische Sicherheit bei einer fortgeschrittenen elektronischen Signatur (die oftmals die Form einer digitalen, zertifikatsbasierten, elektronischen Signatur vorweist) grundsätzlich höher eingestuft wird als bei bestimmten gesetzlich anerkannten, einfachen elektronischen Signaturen wie PIN-Codes oder eingescannten Unterschriften, die einem Dokument beigefügt werden. Grundsätzlich gelten fortgeschrittene elektronische Signaturen somit als vertrauenswürdiger und haben als Beweismittel in einem Gerichtsverfahren im Allgemeinen mehr Gewicht. Aus rechtlicher Sicht darf die jeweils verwendete technische Methode nur eines der Elemente darstellen, die das Gericht im Rahmen seines Ermessens berücksichtigen kann. Daher kann in einem Fall die Vertrauenswürdigkeit einer speziellen zertifikatsbasierten, elektronischen Signatur also möglicherweise in Frage gestellt werden, während das Gericht in einem anderen Fall einen PIN-Code bereits als ausreichenden Beweis ansehen mag.

Auch wenn eine fortgeschrittene elektronische Signatur keine konkrete Rechtswirkung entfaltet, gilt sie grundsätzlich als vertrauenswürdiger und hat als Beweismittel in einem Gerichtsverfahren mehr Gewicht. Zudem lässt die eIDAS-Verordnung offensichtlich Raum für die Möglichkeit, auch elektronische Signaturen, die nicht auf einem digitalen Zertifikat beruhen, als fortgeschrittene elektronische Signaturen einzustufen.

2.4 Qualifizierte elektronische Signaturen

Der handschriftlichen Unterschrift gleichgestellt – Die „qualifizierte elektronische Signatur“ wird in Artikel 3 (12) der eIDAS-Verordnung als eine fortgeschrittene elektronische Signatur definiert, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und die auf einem qualifizierten Zertifikat für elektronische Signaturen beruht.

Ein Schlüsselprinzip der eIDAS-Verordnung besagt, dass gemäß Artikel 25.2 eine qualifizierte elektronische Signatur automatisch einer handschriftlichen Unterschrift gleichzustellen ist und die gleichen Rechtwirkungen entfaltet wie diese. In Artikel 25.3 heißt es zudem, dass eine qualifizierte elektronische Signatur, die auf einem in einem EU-Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, in allen anderen EU-Mitgliedstaaten als qualifizierte elektronische Signatur anzuerkennen ist. Insofern überwindet Artikel 25.3 die mangelnde Interoperabilität, von der die Richtlinie 1999/93/EC für elektronische Signaturen geprägt war, und ermöglicht aufgrund der nunmehr verstärkten rechtlichen Anerkennung von qualifizierten elektronischen Signaturen in den einzelnen EU-Mitgliedstaaten eine sichere und nahtlose Abwicklung grenzüberschreitender elektronischer Transaktionen.

Umfangreicher Kriterienkatalog – Um als qualifizierte elektronische Signatur gelten zu können, muss eine elektronische Signatur auf einem qualifizierten Zertifikat beruhen. Bei einem „qualifizierten Zertifikat“ handelt es sich um ein digitales Zertifikat, das die in Anhang I zur eIDAS-Verordnung aufgeführten konkreten Informationen enthält und von einem qualifizierten Vertrauensdiensteanbieter (nach Verifizierung der Identität und gegebenenfalls besonderer Merkmale der betreffenden natürlichen Person) ausgestellt wird. Ein qualifizierter Vertrauensdienst ist ein Dienstleister, der qualifizierte Vertrauensdienste entsprechend den in Abschnitt 3 der eIDAS-Verordnung niedergelegten Anforderungen erbringt. In der Praxis wird damit im Hinblick auf qualifizierte elektronische Signaturen die gewerbliche oder staatliche Zertifizierungsstelle bezeichnet, die durch Ausstellung eines digitalen Zertifikats bestätigt, dass die genannte Person im Besitz des entsprechenden öffentlichen Schlüssels ist.

Eine qualifizierte elektronische Signatur muss zudem durch eine qualifizierte elektronische Signaturerstellungseinheit erstellt werden. Das bedeutet, dass eine konfigurierte Software oder Hardware (z. B. eine Smartcard, ein USB-Stick oder ein Cloud-basiertes Sicherheitsmodul), die für die Erstellung der besagten Signatur verwendet werden, die Anforderungen an die Vertrauenswürdigkeit der von der Einheit verwalteten Daten, wie in Anhang II zur eIDAS-Verordnung niedergelegt, erfüllen müssen.

Eine qualifizierte elektronische Signatur entfaltet automatisch die gleiche Rechtswirkung wie eine handschriftliche Unterschrift und muss in anderen EU-Mitgliedstaaten anerkannt werden.

2.5 Wirksamkeit und Durchsetzbarkeit elektronischer Vereinbarungen

Wenn man die Verwendung elektronischer Signaturen im Zusammenhang mit vertraglichen Vereinbarungen untersucht, stellt die Frage nach der rechtlichen Wirksamkeit einer elektronischen Signatur nur einen zu klärenden Aspekt dar. Es ergeben sich zwei weitere, gleichermaßen wichtige Fragen. Die erste bezieht sich auf die Wirksamkeit einer elektronisch unterzeichneten Vereinbarung. Die zweite Frage betrifft die Beweiskraft und die Durchsetzbarkeit elektronisch unterzeichneter Vereinbarungen.

Wirksamkeit – Die erste Frage, die es zu beantworten gilt, betrifft die formalen Anforderungen, die erfüllt werden müssen, um eine entsprechende Vereinbarung wirksam abschließen zu können. Im europäischen Vertragsrecht gilt das Grundprinzip der *Einigung*. Das bedeutet, dass die aus freien Stücken gegenseitig erteilten Einwilligungen der Vertragsparteien genügen, damit eine wirksame Vereinbarung zustande kommt.

Weitere formale Voraussetzungen, wie Schriftform des Dokuments, Registrierung oder Unterschriften, müssen nicht erfüllt werden.

Vereinbarungen können mündlich, schriftlich, elektronisch und sogar konkludent abgeschlossen werden. In den verschiedenen EU-Mitgliedstaaten bestehen jedoch mitunter Ausnahmen von dieser allgemeinen Regel. Für Immobilienverträge, öffentliche Vergabeverträge, Verbraucherverträge, Vergleichsvereinbarungen oder Bürgschaftsvereinbarungen können gegebenenfalls spezielle Formvorschriften gelten, die erfüllt werden müssen, um den entsprechenden Vertrag wirksam abschließen zu können. Wenngleich solche Ausnahmen tatsächlich existieren, reichen in den allermeisten Fällen die Einwilligungen der Vertragsparteien aus und es sind für einen wirksamen Vertragsabschluss keine Unterschriften erforderlich.

Durchsetzbarkeit – Die zweite Frage, die es zu beantworten gilt, betrifft die Art und Weise, wie Vereinbarungen wirksam durchgesetzt werden können. Aus rechtlicher Sicht ist diese zweite Frage äußerst relevant, da ein großer Unterschied besteht zwischen dem Abschluss einer wirksamen Vereinbarung und der Möglichkeit, diese Vereinbarung tatsächlich auch durchsetzen zu können, indem man deren Vorliegen und Inhalt beweist.

Die rechtlichen Regeln für die Beweiskraft und die Durchsetzbarkeit von Vereinbarungen unterscheiden sich in den verschiedenen Rechtsordnungen. In Ländern mit Zivilrechtssystemen wie Belgien, Frankreich oder Italien, die beispielhaft für die in Mitteleuropa geltenden Beweisregeln stehen, unterscheidet man zwischen freien und gesetzlich festgelegten Beweisen. Bei Streitigkeiten zwischen Unternehmen sind alle Arten von Beweisen (z. B. schriftliche Beweise, Zeugenbeweise, E-Mails oder faktische Beweise jeglicher Art) zulässig. Natürlich bleibt es jeweils dem Gericht überlassen, die Beweiskraft der vorgelegten Beweise im Einzelfall zu würdigen. Bei Streitigkeiten zwischen Unternehmen und Privatpersonen und bei Streitigkeiten zwischen Privatpersonen sind die zulässigen Beweisformen gesetzlich geregelt. Das heißt, dass bei einem Streitwert, der einen gewissen Betrag übersteigt, die Vereinbarung in der Regel in Schriftform vorgelegt werden muss (also als schriftliches, mit den Unterschriften der beiden sich verpflichtenden Parteien versehenes Dokument), damit eine Durchsetzung möglich wird.

In den meisten Rechtsordnungen dürfen die Beweisvorschriften jedoch vertraglich abbedungen werden. Das heißt, die Vertragsparteien können vereinbaren, welche Beweismittel ausreichen sollen und/oder welche Beweiskraft bestimmten Dokumenten beigemessen werden soll. Ein typisches Beispiel dafür liefern die Geschäftsbedingungen der Online-Banking-Dienste, die vom Nutzer oftmals die Zustimmung verlangen, dass eine durch einen Kartenleser bestätigte Transaktion als elektronische Signatur gelten soll, welche die funktionellen Anforderungen an eine handschriftliche Unterschrift erfüllt.

Darüber hinaus ist zu betonen, dass die Beweisregeln sogar in Fällen, in denen eine bestimmte Beweisart gesetzlich vorgeschrieben ist (beispielsweise die Vorlage einer unterzeichneten Vereinbarung), grundsätzlich auch freien Beweisen eine gewisse Beweiskraft zuerkennen (z. B. E-Mails, die den Inhalt einer Vereinbarung beschreiben), sei es aufgrund einer gesetzlichen Grundlage oder in der Praxis.

Wenngleich zwischen den einzelnen EU-Mitgliedstaaten Unterschiede bestehen, kann durchaus davon ausgegangen werden, (i) dass Vereinbarungen für ihre Wirksamkeit in den allermeisten Fällen keinen formellen Voraussetzungen genügen müssen und (ii) dass bei Streitigkeiten in den meisten Fällen jede Art von Beweis (z. B. jede Art von elektronischer Signatur) zulässig ist, um die Durchsetzbarkeit einer Vereinbarung zu beweisen.

3 Beurteilung der Gesetzeskonformität von Adobe Sign

3.1 Beschreibung von Adobe Sign

Die Cloud-Lösung – Adobe Sign ist eine SaaS-basierte elektronische Signaturlösung mit Workflow, die es dem Nutzer erlaubt, die Unterzeichnung von Dokumenten flexibel zu handhaben. Adobe Sign deckt alle Aspekte des elektronischen Signaturverfahrens ab, von der Bereitstellung von Optionen zur Nutzervalidierung bis hin zur Einbettung der Zustimmung in das endgültige Dokument und der Besiegelung des Dokuments durch eine Originalitätszertifizierung. In jeder Phase des Prozesses übernimmt Adobe Sign die Nutzerverifizierung und verbindet alle Prüfungsinformationen des Unterzeichners mit dessen Signatur unter dem Dokument. Adobe Sign kann über einen Webbrowser, ein mobiles Gerät, über Adobe Acrobat oder über die API-Integration in einer Geschäftsanwendung oder MS Office/MS Sharepoint gestartet und genutzt werden.

Das Signaturverfahren – Um ein Dokument zur Unterzeichnung zu übersenden, lädt der Nutzer das Dokument in Adobe Sign hoch. Adobe Sign unterstützt zahlreiche Formate von Quelldokumenten, die elektronisch unterzeichnet werden können. Der Nutzer kann eine oder mehrere Parteien angeben, die das Dokument unterzeichnen sollen, den Teilnehmern eine Nachricht zukommen lassen und optional das Dokument zusätzlichen Sicherheitskontrollen unterziehen. Adobe Sign ermöglicht es dem Nutzer zudem, in einem Dokument mithilfe einer einfachen Web-Schnittstelle per Drag-and-Drop-Funktion Formular- oder Unterschriftsfelder manuell zu erstellen. Die Unterzeichner werden während des Signaturverfahrens aufgefordert, die notwendigen Felder auszufüllen und an den entsprechenden Stellen eine Unterschrift zu leisten.

Authentifizierung – Adobe Sign unterstützt eine Reihe von Optionen zur Verifizierung der Identität des Nutzers von Adobe Sign und der Unterzeichner.

Der Nutzer von Adobe Sign authentifiziert sich selbst durch eine eindeutige Nutzerkennung, die der Nutzer entweder selbst erstellt oder die der Administrator (im Fall von Unternehmenskonten) ihm zuweist. Der Nutzer kann sich selbst einloggen und durch folgende Kennungsarten authentifizieren:

- Adobe Sign ID – Der Nutzer verwendet eine verifizierte Kombination aus E-Mail-Adresse und Passwort, um sich sicher in seinen Account einzuloggen. Die Account-Administratoren einer Organisation können für das Nutzerpasswort zusätzliche Anforderungen festlegen (z. B. eine Mindestkomplexität oder Anzahl von Zeichen).

- Adobe ID – Der Nutzer kann eine Adobe ID verwenden, um sich in Adobe Sign einzuloggen. Eine Adobe ID ist eine Kennung, die für alle Adobe-Dienste verwendet wird und die den Zugang zu den entsprechenden Diensten ermöglicht. Organisationen können flexibel bestimmen, ob ihre Nutzer sich mit einer Adobe ID in Adobe Sign einloggen können.

- Google Gmail und Google Apps – Adobe Sign unterstützt auch ein Login der Nutzer über einen Google Gmail- oder Google Apps-Account. Die Account-Administratoren können bestimmen, ob die Nutzer diese Methode anwenden können.

- Single-Sign-on (SSO) unter Verwendung der Security Assertion Markup Language (SAML) – Unternehmen, die einen strengeren Zugangskontrollmechanismus beanspruchen, können SAML SSO aktivieren, um ihre Nutzer zentral über das unternehmenseigene Identifizierungssystem zu verwalten. Das ermöglicht den Account-Administratoren, strenge Zugangskontrollen einzuführen und sicherzustellen, dass die Passwortanforderungen mit den jeweiligen Unternehmensrichtlinien für Informationssicherheit in Einklang stehen.

Darüber hinaus unterstützt Adobe Sign verschiedene Optionen für die Identifizierung eines Unterzeichners – der nicht notwendigerweise ein Nutzer von Adobe Sign sein muss und sich nicht zuerst bei Adobe Sign registrieren muss –, der auf diese Weise vor der Unterzeichnung eines Dokuments verifiziert werden kann.

Eine einfache Authentifizierung erfolgt durch Versenden einer E-Mail mit einer eindeutigen URL an einen Unterzeichner. Da die meisten Unterzeichner einen eindeutigen Zugang zu einem E-Mail-Account haben, gilt dies als die erste Ebene der Authentifizierung. Der für die Unterzeichnung des Dokuments benötigte URL-Link setzt sich aus eindeutigen Kennungen zusammen, die speziell für die konkrete Transaktion gelten und die vom Nutzer von Adobe Sign passwortgeschützt werden können. Nach Anklicken des besagten URL-Links können die Unterzeichner mithilfe einer Maus oder eines vorher eingestellten Schrifttyps auf dem Bildschirm eine ‚handschriftliche' Signatur erzeugen, eine bestehende Datei hochladen (z. B. eine gescannte Unterschrift), ihren Namen eintippen und zum Unterzeichnen einen Button anklicken (der anzeigt: „Zum Unterschreiben klicken").

Darüber hinaus erlaubt Adobe Sign eine mehrstufige Authentifizierung und bietet weitere Authentifizierungsmechanismen, um die Identität eines Unterzeichners feststellen zu können, beispielsweise eindeutige Passwörter für die einzelnen Unterzeichner, eine telefonische Authentifizierung (durch Stimme oder SMS) oder eine Social-Media-Identifizierung über den Account des jeweiligen Unterzeichners bei Facebook oder Google.

Dokumentenzertifizierung – Nachdem die Unterzeichner das Dokument unterzeichnet haben, zertifiziert Adobe Sign das Dokument, damit etwaige Änderungen erkennbar werden. Adobe Sign implementiert eine eigene PKI. Diese ist mit dem Programm Adobe Approved Trust List (AATL) kompatibel, das die Dokumentenzertifizierung unterstützt. Adobe Sign zertifiziert automatisch eine endgültige PDF-Datei des unterzeichneten Dokuments, bevor diese allen Teilnehmern zugeleitet wird. Wenn die Empfänger die unterzeichnete Datei in Adobe Acrobat oder Acrobat Reader herunterladen, erscheint an der Kopfseite des Dokuments ein blaues Banner, das bestätigt, dass keine nichtautorisierte Quelle das Dokument während des Übermittlungsvorgangs oder zu irgendeinem Zeitpunkt nach Anbringen der Zertifizierung manipuliert hat.

Nachdem alle Unterzeichner das Dokument unterzeichnet haben, speichert Adobe Sign automatisch alle unterzeichneten Dokumente in einem zentralisierten, sicheren Speicher, wo sie leicht zugänglich sind. Die Nutzer können aber auch wählen, die Dienste in ihre eigenen bestehenden Lösungen für Dokumenten-Management zu integrieren.

Prüfprotokoll – Adobe Sign ermöglicht Echtzeit-Transparenz im Signaturverfahren. Sobald das Dokument zur Unterzeichnung losgeschickt worden ist, regelt Adobe Sign automatisch den Workflow, die Überwachung, das Tracking, die Erinnerungen und die Authentifizierung, um auf diese Weise das elektronische Signaturverfahren klar und einfach zu gestalten.

Jeder wichtige Schritt des Signaturverfahrens wird mit einem Zeitstempel protokolliert. Dieses Protokoll enthält beispielsweise Informationen darüber, wann das Dokument versendet, geöffnet und unterzeichnet wurde, sowie die IP-Adressen beziehungsweise bei Nutzung der mobilen App den Standort der Unterzeichner und zudem die jeweilige spezielle Form der Authentifizierung, die für jeden einzelnen Unterzeichner und für jede einwilligende Partei verwendet wird. Das Ergebnis wird in einem sicheren, zertifizierten Prüfprotokoll festgehalten, der einen eindeutigen und leicht abrufbaren Nachweis der Unterschrift jedes einzelnen Unterzeichners liefert. Das Prüfprotokoll kann der Nutzer von Adobe Sign über das Adobe Sign Dashboard abrufen. Ein Unterzeichner (der nicht der Nutzer ist) kann Zugang zum Prüfprotokoll erhalten, indem er auf eine Unterschrift in dem unterzeichneten Dokument klickt.

Digitale Signaturen – Adobe Sign erlaubt nicht nur die Erstellung elektronischer Signaturen, die nicht auf einem digitalen Zertifikat beruhen, sondern unterstützt auch die Verwendung von digitalen, zertifikatsbasierten Signaturen durch Verwendung von Adobe Sign in Verbindung mit Adobe Acrobat oder Adobe Reader, um auf diese Weise digitale Signaturen auf Dokumenten zu erfassen. Während des Signaturverfahrens wird das Zertifikat des Unterzeichners mithilfe des privaten Schlüssels des entsprechenden Unterzeichners kryptografisch mit dem Dokument verbunden. Während des Validierungsprozesses wird der reziproke öffentliche Schlüssel aus der Unterschrift extrahiert und sowohl zur Authentifizierung der Identität des Unterzeichners als auch zur Sicherstellung herangezogen, dass an dem Dokument nach der Unterzeichnung keine Änderungen vorgenommen wurden. In diesem Zusammenhang liefert das Prüfprotokoll zusätzliche wertvolle Informationen wie beispielsweise die IP-Adresse, Zeitstempel oder bei App-Nutzung den Standort des Unterzeichners (Zustimmung erforderlich).

Adobe ist kein Trustcenter. Infolgedessen stellt Adobe Sign selbst keine digitalen Zertifikate aus, verarbeitet aber über 250 digitale Zertifikate, die von Drittdienstleistern oder eIDAS-autorisierten Trustcentern ausgestellt wurden. Fast alle dieser Dienstleister werden von Adobe Sign durch Aufnahme in die EUTL (European Trustcenter List) und in der AATL Adobe Approved Trust List anerkannt (diese Liste enthält beispielsweise Vertrauensdienste wie DigiCert, GlobalSign, QuoVadis etc.).

Cloud-Sicherheit – Adobe hat eine Reihe von technischen und organisatorischen Maßnahmen in Bezug auf die physische Sicherheit des Rechenzentrums, Disaster Recovery, Umgebungskontrollen, logische Sicherheit, Datenschutz, Intrusion Detection, Reaktion und Überwachung umgesetzt, um auf diese Weise die Sicherheit von Adobe Sign und der damit verbundenen Prozesse zu gewährleisten. Geschäftsprozesse mit Adobe Sign sind nach ISO 270001, SSAE SOC 2 Typ 2 und PCI DSS zertifiziert.

Abonnements – Adobe Sign kann im Rahmen von drei verschieden Abonnements verwendet werden: „Einzelanwender“, „Business“ und „Unternehmen“. Der Funktionsumfang hängt vom gewählten Abonnement ab. Die mehrstufige Authentifizierung steht zum Beispiel nur bei den Abonnements „Business“ und „Unternehmen“ zur Verfügung, während die Verwendung digitaler, zertifikatsbasierter, elektronischer Signaturen nur beim Abonnement „Unternehmen“ möglich ist.

3.2 Wie Adobe Sign die Einhaltung von eIDAS unterstützen kann

In diesem Abschnitt wird geprüft, inwieweit Adobe Sign die oben dargelegten gesetzlichen Anforderungen an einfache, fortgeschrittene und qualifizierte elektronische Signaturen berücksichtigt.

3.3 Adobe Sign erfüllt die europäischen Anforderungen für einfache elektronische Signaturen

Anforderungen – Entsprechend der Definition von einfachen elektronischen Signaturen in der eIDAS-Verordnung müssen in elektronischer Form vorliegende Daten mit anderen Daten in elektronischer Form verbunden und logisch verknüpft sein und vom Unterzeichner für seine Unterschrift verwendet werden.

Adobe Sign – Angesichts der oben gegebenen Beschreibung von Adobe Sign gehen wir davon aus, dass Adobe Sign aus rechtlicher Sicht die Anforderungen an einfache elektronische Signaturen erfüllt und darüber hinausgeht:

- *„Daten in elektronischer Form“* – Elektronische Signaturen, die mit Adobe Sign erstellt werden, bestehen tatsächlich aus Datenketten in elektronischer Form.

- *„anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden“* – Die elektronische Signatur kann vom Unterzeichner mit einer Vielzahl von elektronischen Dokumenten verbunden werden, wobei Adobe Sign das Hochladen unterschiedlichster Quelldokumentformate erlaubt.

- *„vom Unterzeichner für seine Unterschrift verwendet“* – Adobe Sign wurde mit einer klaren Ausrichtung darauf konzipiert, die Absicht des Unterzeichners zur Unterschrift in einem Signaturverfahren zu erfassen:

  - Der Unterzeichner erhält eine E-Mail mit dem Betreff „Bitte unterzeichnen Sie [Name des Dokuments]“, die einen Hyperlink zu Adobe Sign enthält, der lautet: „Hier klicken, um [Name des Dokuments] zu prüfen und zu unterzeichnen“;

  - Wenn der Unterzeichner das Dokument prüft, wird er aufgefordert, das Dokument zu unterzeichnen, indem er seinen Namen eintippt und so auf dem Bildschirm eine ‚handschriftliche‘ Unterschrift erzeugt oder das Bild seiner gescannten Unterschrift hochlädt. Der Unterzeichner wird dazu durch ein Formularfeld mit der Anweisung „Zum Signieren hier klicken“ aufgefordert;

  - Sobald das geschehen ist, erscheinen die Mitteilung „Ich stimme den allgemeinen Geschäftsbedingungen und den wichtigen Informationen für Verbraucher betreffend dieses Dokuments zu“ sowie ein Button mit der Aufforderung „Anklicken, um zu unterschreiben“. Erst wenn der Unterzeichner diesen Button anklickt und seine Absicht zur Unterzeichnung ein zweites Mal bestätigt hat, betrachtet Adobe Sign das Dokument als unterzeichnet und leitet es an die anderen Teilnehmer weiter.

Wenngleich die Unterschrift auf dem Dokument nur als visuelles, ästhetisches Merkmal ohne Auswirkung auf den Wert der elektronischen Signatur erscheint, wird aufgrund der mehrstufigen Methode zur Erfassung der Unterzeichnungsabsicht des Unterzeichners dieses dritte Kriterium erfüllt. Hierbei geht es nicht nur um die Anforderung, einfache elektronische Signaturen zu erstellen, sondern um einen wichtigen Aspekt des Vertragsschlusses. Da Verträge grundsätzlich durch gegenseitige Einwilligungen der Vertragsparteien abgeschlossen werden, hilft ein klar strukturiertes Signaturverfahren dabei, die Bereitschaft des jeweiligen Unterzeichners, sich durch rechtliche Verpflichtungen binden zu wollen, zu beweisen und daraus dessen diesbezügliche Einwilligung abzuleiten.

Gemäß Artikel 25.1 der eIDAS-Verordnung bedeutet dies, dass einer mithilfe von Adobe Sign erstellten elektronischen Signatur die rechtliche Wirksamkeit und die Zulassung als Beweismittel in einem Gerichtsverfahren grundsätzlich nicht allein aufgrund ihrer technischen Merkmale versagt werden können. Das bedeutet jedoch nicht, dass eine solche elektronische Signatur automatisch die gleiche rechtliche Wirksamkeit entfaltet wie eine handschriftliche Unterschrift, es sei denn, ein qualifiziertes Zertifikat wird verwendet (siehe nachstehend unter Ziffer 3.2.3).

Adobe Sign bietet darüber hinaus eine Reihe von Funktionen, welche die Durchsetzbarkeit als elektronische Signatur, vergleichbar mit anderen, allgemein anerkannten elektronischen Signaturen, stärken könnten. Dazu zählen:

- Das Prüfprotokoll – Wird die Wirksamkeit der elektronischen Signatur angefochten, so kann das von Adobe Sign generierte Prüfprotokoll als maßgeblicher Beweis dienen, der die Verbindung zwischen der Identität des Unterzeichners und der Unterschrift über Zeitstempel und IP-Adresse belegt.

- Die mehrstufigen Authentifizierungsmethoden – Wird vom Unterzeichner durch Auswahl bestimmter Einstellungen eine mehrstufige Authentifizierung verlangt, erhöht dies unweigerlich die Möglichkeit für eine ordnungsgemäße Authentifizierung des Unterzeichners und für die Erstellung von elektronischen Signaturen mit erhöhter Beweiskraft.

Aus den obigen Ausführungen lässt sich der Schluss ziehen, dass Adobe Sign nicht nur eine Lösung für die Erstellung einfacher, mit der eIDAS-Verordnung konformer elektronischer Signaturen bietet, sondern dass mit Adobe Sign auch eine vertrauenswürdige und sichere Methodik zur Verfügung steht.

Adobe Sign ermöglicht die Erstellung von einfachen elektronischen Signaturen mithilfe einer vertrauenswürdigen und sicheren Methodik. Adobe Sign (i) ermöglicht die Identifizierung der Unterzeichner auf fortschrittliche Weise, (ii) erfasst die Unterzeichnungsabsicht auf eindeutige Weise und (iii) verwaltet Prüfprotokolle, um die Durchsetzbarkeit elektronischer Signaturen zu unterstützen.

3.4 Adobe Sign und fortgeschrittene elektronische Signaturen

Anforderungen – Entsprechend der Definition von fortgeschrittenen elektronischen Signaturen in der eIDAS-Verordnung müssen diese elektronischen Signaturen eindeutig dem Unterzeichner zugeordnet sein, die Identifizierung des Unterzeichners ermöglichen, unter Verwendung elektronischer Signaturerstellungsdaten erstellt sein, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann und so mit den auf diese Weise unterzeichneten Daten verbunden sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Adobe Sign – Angesichts der oben enthaltenen Beschreibung von Adobe Sign gehen wir davon aus, dass Adobe Sign aus rechtlicher Sicht die Erstellung digitaler, zertifikatsbasierter, fortgeschrittener elektronischer Signaturen unterstützt:

Wie oben bereits ausgeführt, werden die an fortgeschrittene elektronische Signaturen gestellten Anforderungen in der Regel durch digitale, zertifikatsbasierte, elektronische Signaturen erfüllt. Adobe generiert und verwaltet jedoch keine Zertifikate für die Erstellung solcher Signaturen. Allerdings weist Adobe Sign mit Adobe Acrobat und Acrobat Reader eine integrierte Funktion vor, welche die Erstellung sogenannter „digitaler Signaturen“ ermöglicht. Zur Klarstellung muss betont werden, dass das Konzept einer „digitalen Signatur“, so wie Adobe Sign es verwendet, in der eIDAS-Verordnung nicht rechtlich definiert wird. Es muss jedoch so ausgelegt werden, dass es digitale, zertifikatsbasierte, fortgeschrittene elektronische Signaturen, qualifizierte elektronische Signaturen sowie elektronische Signaturen, die auf selbstunterzeichneten Zertifikaten beruhen, einschließt.

Wenn ein Dokument zur Unterzeichnung in Adobe Sign hochgeladen wird, kann der Adobe Sign-Nutzer von den Unterzeichnern verlangen, eine digitale Signatur zu verwenden, indem er ein Formularfeld für eine digitale Signatur in das Dokument einfügt. Die Unterzeichner werden daraufhin dazu aufgefordert, das Dokument herunterzuladen, das sich sodann (je nach Einstellungen auf dem Computer des Unterzeichners) in Adobe Acrobat oder Acrobat Reader öffnet. Der Unterzeichner wird zum Unterschriftsfeld geführt. Er kann ein auf seinem Gerät gespeichertes Zertifikat auswählen und die fortgeschrittene elektronische Signatur über Adobe Acrobat oder Acrobat Reader dem Dokument hinzufügen. Das unterzeichnete Dokument wird dann automatisch in Adobe Sign hochgeladen (ohne weiteren Handlungsbedarf aufseiten des Unterzeichners), die anderen Unterzeichner werden benachrichtigt und die digitale Signatur wird im Prüfprotokoll für das Dokument festgehalten. Auch wenn das Prüfprotokoll lediglich bestätigt, dass das Dokument digital unterzeichnet wurde, können der Nutzer von Adobe Sign sowie die Unterzeichner die Wirksamkeit des verwendeten

digitalen Zertifikats prüfen, indem sie das unterzeichnete Dokument in Adobe Sign aufrufen oder es direkt in Acrobat Reader oder Adobe Acrobat öffnen.

Digitale, zertifikatsbasierte, fortgeschrittene elektronische Signaturen können in ein durchgängiges Signaturverfahren integriert werden, das von Adobe Sign unterstützt und verwaltet wird.

Wie oben in Ziffer 2.1.2 dargelegt, lässt sich argumentieren, dass bestimmte Signaturtechnologien, mit Ausnahme der mit öffentlichen Schlüsseln operierenden Kryptografie, wie zum Beispiel prozessfokussierte, Cloud-basierte elektronische Signaturlösungen, in der Lage sein können, die Anforderungen an fortgeschrittene elektronische Signaturen zu erfüllen. Daher soll an dieser Stelle die Funktion „digitale Signatur" außer Acht gelassen werden und die Lösung in Bezug auf die vier für fortgeschrittene elektronische Signaturen aufgestellten Kriterien gewürdigt werden. Dabei ergibt sich Folgendes:

- *„eindeutig dem Unterzeichner zugeordnet"* – Adobe Sign ermöglicht es, jede über die Plattform erstellte elektronische Signatur einem Unterzeichner zuzuordnen. Adobe Sign bietet mehrstufige Authentifizierungsmethoden, um Unterzeichner eindeutig authentifizieren zu können. Zusätzlich lässt sich anhand des Prüfprotokolls, das alle elektronischen Signaturen in einem Dokument erfasst, jede einzelne Unterschrift einem bestimmten Unterzeichner zuordnen.

- *„die Identifizierung des Unterzeichners ermöglichen"* – Um sicherzustellen, dass diese Anforderung erfüllt ist, wird den Nutzern geraten, für das Login und die Unterzeichnung des Dokuments eine mehrstufige Authentifizierung anzufordern, anstatt den Zugang lediglich durch Anklicken eines Hyperlinks zu gestatten.

- *„unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann"* – Normalerweise gelten nur digitale, zertifikatsbasierte, fortgeschrittene elektronische Signaturen als geeignet, dieses Kriterium zu erfüllen, wobei der private Schlüssel des jeweiligen Unterzeichners als „elektronische Signaturerstellungsdaten" zu betrachten ist. Das Konzept „elektronische Signaturerstellungsdaten" beschränkt sich jedoch nicht notwendigerweise auf private Schlüssel, da die eIDAS-Verordnung hierzu eine weitgefasste Definition enthält und von „eindeutigen Daten, die vom Unterzeichner zum Erstellen einer elektronischen Signatur verwendet werden", spricht.

- Gemäß Erwägungsgrund 52 der eIDAS-Verordnung können auch Cloud-basierte elektronische Signaturlösungen (die nicht notwendigerweise auf digitalen Zertifikaten beruhen) in der Lage sein, dieses Kriterium zu erfüllen, und zwar unter der Voraussetzung, dass spezielle Verwaltungs- und Sicherheitsverfahren eingerichtet und vertrauenswürdige Systeme und Produkte verwendet werden, um zu garantieren, dass die Umgebung für die Erstellung der elektronischen Signatur zuverlässig ist und unter der alleinigen Kontrolle des Unterzeichners steht. Werden für den Zugang zu der personalisierten Unterzeichnungsumgebung und zum Dokument selbst strenge mehrstufige Authentifizierungsmethoden verwendet, so lässt sich argumentieren, dass die Plattform Adobe Sign in der Tat die Erstellung elektronischer Signaturen mit Mitteln ermöglicht, die ein hohes Maß an Vertrauenswürdigkeit genießen und unter der Kontrolle des Unterzeichners stehen. In diesem Zusammenhang sollte darauf hingewiesen werden, dass die Adobe-Administratoren ohne vorherige Zustimmung des Nutzers selbst keinerlei Zugang zu den Nutzer-Accounts, den Profilen der Unterzeichner oder den Login-Daten (einschließlich der Passwörter) haben und somit nicht auf diese Accounts und Profile zugreifen können.

- *„mit den auf diese Weise unterzeichneten Daten derart verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann"* – Nachdem die Unterzeichner das Dokument unterzeichnet haben, zertifiziert

Adobe Sign automatisch das unterzeichnete Dokument durch ein digitales Zertifikat, um das Dokument auf diese Weise vor späteren Veränderungen zu schützen. Sobald ein Dokument mithilfe von Adobe Sign unterzeichnet worden ist, werden spätere Veränderungen zudem leicht erkennbar, da im Prüfprotokoll alle Vorgänge und Veränderungen im Zusammenhang mit dem betreffenden Dokument festgehalten werden.

Es sprechen Argumente dafür, dass Adobe Sign die Erstellung von fortgeschrittenen elektronischen Signaturen ermöglicht, ohne dass diese auf einem digitalen Zertifikat beruhen.

3.5 Adobe Sign und qualifizierte elektronische Signaturen

Anforderungen – Entsprechend der eIDAS-Verordnung ist eine qualifizierte elektronische Signatur einer handschriftlichen Unterschrift gleichzustellen und muss als solche in allen anderen EU-Mitgliedstaaten anerkannt werden. Wie oben bereits dargelegt, definiert die eIDAS-Verordnung eine qualifizierte elektronische Signatur als eine fortgeschrittene elektronische Signatur, mit der zusätzlichen Anforderung, dass diese auf einem qualifizierten Zertifikat für elektronische Signaturen beruhen und von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt worden sein muss.

Die erste Anforderung bezieht sich auf die Verwendung eines qualifizierten Zertifikats. Darunter ist ein digitales Zertifikat zu verstehen, das von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde und die Anforderungen von Anhang I zur eIDAS-Verordnung erfüllt. Was die Anforderungen der eIDAS-Verordnung anbelangt, so entspricht ein Zertifikat, das einen Unterzeichnerschlüssel und die Identität des Inhabers ausweist und durch ein qualifiziertes gewerbliches oder staatliches Zertifikat ausgestellt wurde, der Definition des qualifizierten Zertifikats.

Die zweite Anforderung betrifft die Verwendung einer qualifizierten elektronischen Signaturerstellungseinheit. Unter einer solchen Einheit ist eine konfigurierte Hardware oder Software (z. B. eine Smartcard, ein USB-Stick oder ein Cloud-basiertes Sicherheitsmodul) zu verstehen, die verwendet wird, um eine elektronische Signatur zu erstellen und die den Anforderungen von Anhang II zur eIDAS-Verordnung entspricht.

Adobe Sign – Adobe Sign ermöglicht keine Verwaltung oder Ausstellung von qualifizierten Zertifikaten und stellt auch keine qualifizierten elektronischen Signaturerstellungseinheiten zur Verfügung. Wir gehen allerdings davon aus, dass Adobe Sign aus rechtlicher Sicht die Erstellung qualifizierter elektronischer Signaturen aufgrund seiner Zusammenarbeit mit qualifizierten Zertifikatanbietern unterstützt.

Adobe Sign verfügt mit Adobe Acrobat und Acrobat Reader über eine integrierte Funktion, welche die Erstellung sogenannter „digitaler Signaturen“ ermöglicht. Zur Klarstellung muss betont werden, dass das Konzept einer „digitalen Signatur“, so wie Adobe Sign es verwendet, in der eIDAS-Verordnung nicht rechtlich definiert wird. Es muss jedoch so ausgelegt werden, dass es digitale, zertifikatsbasierte, fortgeschrittene elektronische Signaturen, qualifizierte elektronische Signaturen sowie elektronische Signaturen, die auf selbstunterzeichneten Zertifikaten beruhen, einschließt.

Wenn ein Dokument in Adobe Sign zur Unterschrift hochgeladen wird, kann der Adobe Sign-Nutzer von den Unterzeichnern die Verwendung einer digitalen Signatur verlangen, indem er ein Formularfeld für eine digitale Signatur in das Dokument einfügt. Die Unterzeichner werden daraufhin aufgefordert, das Dokument herunterzuladen, welches sich dann (je nach den Einstellungen auf dem Computer des Unterzeichners) in Adobe Acrobat oder Acrobat Reader öffnet. Der Unterzeichner wird zum Unterschriftsfeld geführt. Er kann ein auf seinem Gerät gespeichertes Zertifikat auswählen und die fortgeschrittene elektronische Signatur über Adobe Acrobat oder Acrobat Reader dem Dokument hinzufügen. Das unterzeichnete Dokument wird dann automatisch in Adobe Sign hochgeladen (ohne weiteren Handlungsbedarf aufseiten des Unterzeichners), die

anderen Unterzeichner werden benachrichtigt und die digitale Signatur wird im Prüfprotokoll für das Dokument festgehalten. Auch wenn das Prüfprotokoll lediglich bestätigt, dass das Dokument digital unterzeichnet wurde, können der Adobe Sign-Nutzer und die Unterzeichner die Wirksamkeit des verwendeten digitalen Zertifikats prüfen, indem sie das unterzeichnete Dokument in Adobe Sign aufrufen oder es direkt in Acrobat Reader oder Adobe Acrobat öffnen.

Da in einigen Fällen die Verwendung qualifizierter elektronischer Unterschriften verlangt wird, um eine Vereinbarung rechtswirksam elektronisch zu unterzeichnen, ist den Nutzern von Adobe Sign und den Unterzeichnern zu empfehlen, jeweils sicherzustellen, dass die entsprechenden Einstellungen aktiviert sind, um eine rechtswirksame Vereinbarung abschließen zu können.

Der Vollständigkeit halber sollte erwähnt werden, dass Adobe Acrobat und Acrobat Reader tatsächlich über bestimmte Funktionen verfügen, um qualifizierte Zertifikate mithilfe einfacher Zertifikatsbestätigungen sowie auf der Grundlage der EU Trusted List (EU-Vertrauensliste) zu identifizieren, um qualifizierte Zertifikate zu verifizieren und diesen aufgrund der EU Trusted List zu vertrauen, um qualifizierte elektronische Signaturerstellungseinheiten mithilfe einfacher Zertifikatsbestätigungen zu identifizieren und um digitale Signaturen im Format PAdES Baseline (sowohl ETSI TS 103 172 als auch das aktuelle ETSI EN 319 142-1) zu unterstützen.

Qualifizierte elektronische Signaturen können in ein durchgängiges Signaturverfahren integriert werden, das von Adobe Sign unterstützt und verwaltet wird.

4 Fazit

Adobe Sign stellt eine SaaS-basierte elektronische Signaturlösung dar, die alle Aspekte des elektronischen Signaturverfahrens abdeckt, von der Bereitstellung von Validierungsoptionen bis hin zur Einbettung der Einwilligung in das endgültige Dokument und der Besiegelung des Dokuments durch eine Originalitätszertifizierung.

Adobe Sign unterstützt eine Reihe von Optionen zur Verifizierung der Identitäten der Nutzer von Adobe Sign und der Unterzeichner und bedient sich dabei spezieller Kennungen (z. B. Adobe Sign ID oder Google Gmail Account) und (mehrstufiger) Authentifizierungsmethoden (z. B. eindeutiger Passwörter, telefonischer Authentifizierung durch Stimme oder SMS oder Social-Media-Identifizierung). Darüber hinaus wurden die Prozesse, die Adobe Sign zugrunde liegen, so konzipiert, dass sie sich eindeutig auf das Erfassen der Absicht der Unterzeichner konzentrieren. Schließlich stellt Adobe Sign zum Schutz des unterzeichneten Dokuments vor nachträglichen Veränderungen auch ein Prüfprotokoll zur Verfügung, welches Aufzeichnungen über alle etwaigen Veränderungen enthält, die an dem unterzeichneten Dokument vorgenommen wurden, und das endgültige Dokument zertifiziert, ehe es an alle Teilnehmer in Umlauf gebracht wird.

Aus rechtlicher Sicht gehen wir davon aus, dass Adobe Sign bei Auswahl der richtigen Benutzereinstellungen ein vertrauenswürdiges und sicheres Tool darstellt, das es ermöglicht, einfache elektronische Signaturen zu erstellen, die den in Artikel 3 (10) der eIDAS-Verordnung formulierten Anforderungen an „einfache elektronische Signaturen“ entsprechen oder sogar darüber hinausgehen. Dies bedeutet, dass man diesen Signaturen gemäß Artikel 25.2 der eIDAS-Verordnung die rechtliche Wirksamkeit nicht alleine aufgrund ihrer technischen Merkmale absprechen kann. Wenngleich eine einfache elektronische Signatur nicht automatisch die gleiche Rechtswirkung entfaltet wie eine handschriftliche Unterschrift, gilt die einfache elektronische Signatur mit Blick auf ihre beabsichtigte Verwendung als einfachere und flexiblere Methode für einen rechtswirksamen Vertragsabschluss sowie hinsichtlich der Durchsetzbarkeit dennoch oftmals als gleichwertig. Wenn Gerichte die Beweiskraft der ihnen vorgelegten Beweise würdigen müssen, werden sie Dokumenten, die mithilfe einer

vertrauenswürdigeren und sichereren Technologie unterzeichnet wurden, in der Regel mehr Gewicht beimessen. In dieser Hinsicht schafft Adobe Sign durch die Bereitstellung einer mehrstufigen Authentifizierung, die Erfassung jeder einzelnen Handlung über Adobe Sign und die Zertifizierung des unterzeichneten Dokuments maßgebliche Beweiskraft.

Darüber hinaus spricht unseres Erachtens einiges dafür, dass Adobe Sign ohne Verwendung einer entsprechenden Technologie für digitale Signaturen die Erstellung „fortgeschrittener elektronischer Signaturen“, wie in Artikel 3 (11) der eIDAS-Verordnung definiert, ermöglicht. Da die eIDAS-Verordnung fortgeschrittenen elektronischen Signaturen keine speziellen Rechtswirkungen zuschreibt, die sich von den Rechtswirkungen einfacher elektronischer Signaturen unterscheiden würden, gilt festzuhalten, dass Adobe Sign als eine vertrauenswürdige und sichere Lösung für elektronische Signaturen betrachtet werden muss, selbst wenn es die rechtlichen Anforderungen an fortgeschrittene elektronische Signaturen nicht erfüllen sollte.

Zudem stellen wir fest, dass Adobe Sign eine Option bietet, welche die Verwendung digitaler Signaturtechnologien unterstützt, insbesondere für digitale, zertifikatsbasierte, fortgeschrittene elektronische Signaturen und „qualifizierte elektronische Signaturen“ wie in Artikel 3 (12) der eIDAS-Verordnung definiert. Bei Aktivierung der entsprechenden Option durch den Nutzer kann Adobe Sign als ein unternehmensfreundliches Tool bezeichnet werden, das die Erstellung fortgeschrittener und qualifizierter elektronischer Signaturen unterstützt und erleichtert. Im Fall von qualifizierten elektronischen Signaturen bedeutet dies, dass Adobe Sign die Erstellung elektronischer Signaturen unterstützt, die gemäß Artikel 25 der eIDAS-Verordnung die gleichen Rechtswirkungen entfalten.

Adobe Sign stellt eine zuverlässige Lösung für elektronische Signaturen dar, die es dem Nutzer erlaubt, den gesamten Unterzeichnungsprozess in einer Weise abzuwickeln, die mit sämtlichen Arten von elektronischen Signaturen, welche die eIDAS-Verordnung vorsieht, kompatibel ist. Adobe Sign erlaubt es dem Nutzer insbesondere, Workflows im Einklang mit seinem individuellen Compliance-, Branchen- und Risikoprofil zu konfigurieren und aufzubauen.

5 Über den Verfasser

Prof. Dr. Patrick Van Eecke ist Partner der Praxisgruppe IT-Recht von DLA Piper in Brüssel, Mitglied der Anwaltskammer Brüssel und außerordentliches Mitglied der amerikanischen Anwaltsvereinigung. Prof. Dr. Van Eecke berät sowohl Behörden als auch Unternehmen im Hinblick auf eine gesetzeskonforme Umsetzung ihrer jeweiligen E-Signatur-Lösungen. Er verfügt über Erfahrungen bei der Erstellung und Aushandlung von PKI-bezogenen rechtlichen Urkunden, wie beispielsweise Erklärungen über Zertifizierungskonzepte, Zertifizierungsrichtlinien, Signaturrichtlinien oder Relying-Party-Verträgen.

Prof. Dr. Patrick Van Eecke engagiert sich intensiv in diversen Forschungs- und Beratungsprojekten für die Europäische Kommission sowie für einige nationale Regierungen. So nahm er bisher beispielsweise an der ersten Studie der Europäischen Kommission über die rechtlichen Aspekte elektronischer Signaturen (1998), der Studie der Europäischen Kommission über Richtlinien für elektronische Signaturen (2001), der Studie der Europäischen Kommission über die langfristige Archivierung elektronischer Signaturen (2001) und der Studie der Europäischen Kommission über die rechtlichen und marktspezifischen Aspekte elektronischer Signaturen (2003) teil. Bei der Studie der Europäischen Kommission über die Zukunft der ICT-Standardisierungsrichtlinie (2006) fungierte er als leitender Berater. In jüngster Zeit war er maßgeblich an der Machbarkeitsstudie der Europäischen Kommission über Richtlinien für elektronische Identifizierung, Authentifizierung und Signaturen (IAS) (2010) sowie an einer Studie der Europäischen Kommission über die Umsetzung eines paneuropäischen Rahmenwerks für elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (2014) beteiligt.

Prof. Dr. Van Eecke nahm als nationaler Repräsentant an Debatten des Europäischen Rates über die Richtlinie für elektronische Signaturen und die Richtlinie für Electronic Commerce teil. Zudem beriet er den Wirtschafts- und Sozialausschuss der Europäischen Gemeinschaften in den genannten Angelegenheiten. Als rechtlicher Sachverständiger im Expertenteam EESSI (Europäische Initiative für die Standardisierung elektronischer Signaturen) war er Mitverfasser des ersten EESSI-Berichts und daraus sich ergebender rechtlicher Ergebnisse.

Prof. Dr. Van Eecke erwarb seinen Doktortitel an der Universität Leuven (einschließlich eines Gaststipendiums an der Universität Stanford) und promovierte zum Thema „Der rechtliche Status elektronischer Signaturen“ (2003). Er ist Professor an der Universität Antwerpen und lehrt dort europäisches Informations- und Kommunikationsrecht. Außerdem unterrichtet er am Kings College und an der Queen Mary Universität (London) als Gastdozent. Prof. Dr. Van Eecke ist Autor zahlreicher juristischer Artikel und Bücher zu den Themen Computer-Kriminalität, elektronische Signaturen, elektronische Vertragsabschlüsse und Datenschutz. Er tritt regelmäßig als Referent bei nationalen und internationalen Konferenzen auf.

www.dlapiper.com