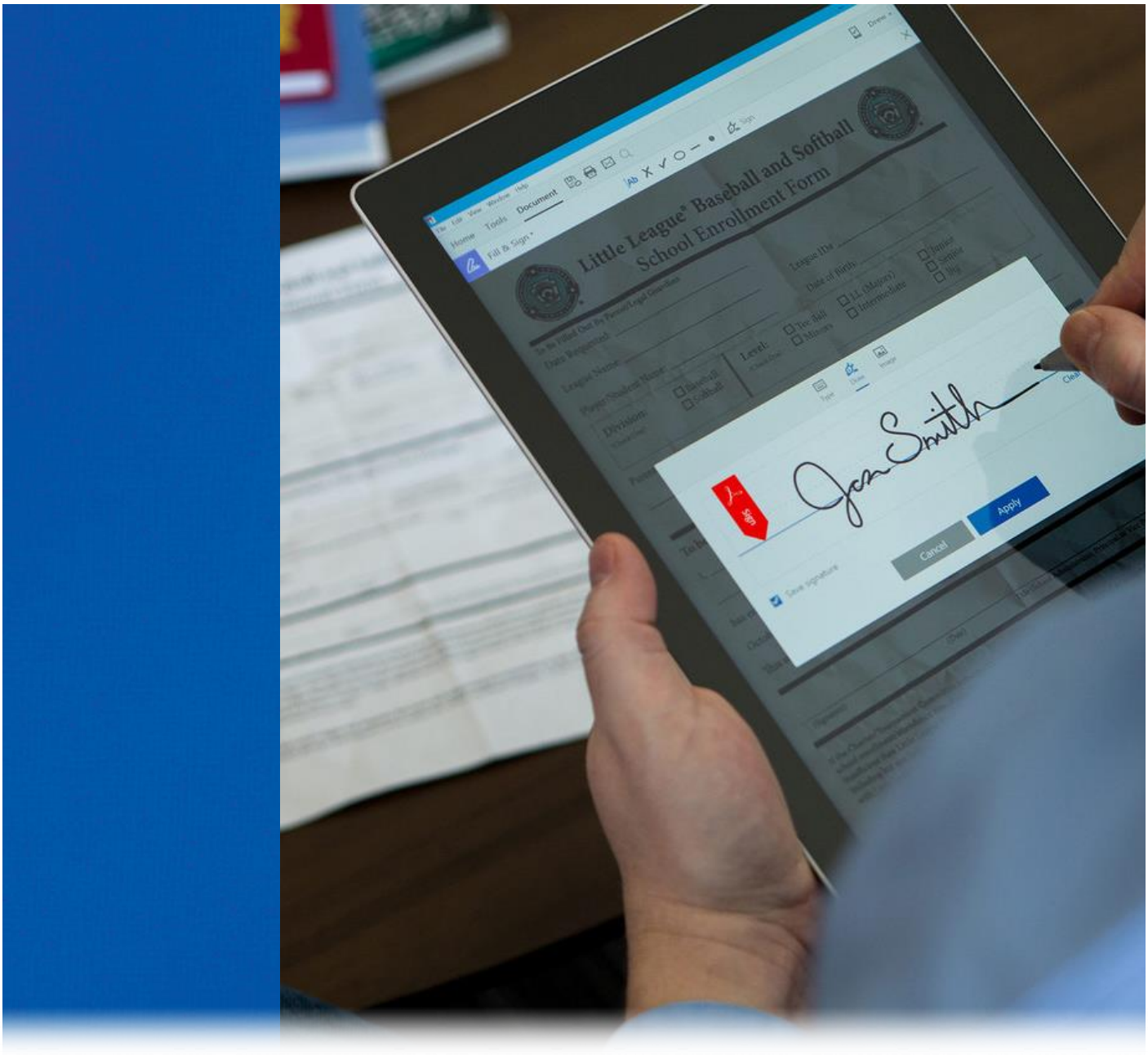

ADOBE SIGN

Compliance with European electronic signatures legislation

December 2016

DLA PIPER

Adobe

TABLE OF CONTENTS

1 INTRODUCTION

This white paper assesses the legal effectiveness of the Adobe Sign solution in relation to European requirements applicable to electronic signatures. In the first part of this white paper, we give an overview of the relevant legal framework. We briefly describe the scope, main concepts and legal consequences of Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (hereafter **"eIDAS Regulation"** or **"Regulation"**), which is the core instrument governing the validity of electronic signatures in the EU. We will further analyse key questions related to the validity and enforceability of electronically signed agreements.

In the second part, this white paper describes the key features of Adobe Sign and reviews those key features in regard of the relevant legal requirements with the aim to analyse the legally binding nature of electronic signatures produced with Adobe Sign.

We conclude that when the appropriate user settings are selected, from a legal perspective, Adobe Sign is a trustworthy and secure tool that allows one to produce electronic signatures that meet or even exceed the requirements of an electronic signature as defined in Article 3 (10) of the eIDAS Regulation.

Moreover, we believe that arguments exist to state that Adobe Sign, without the use of digital signature technology, may allow one to produce advanced electronic signatures as defined in Article 3 (11) of the eIDAS Regulation.

Furthermore, we observe that Adobe Sign also contains an option supporting the use of digital signature technology, notably digital certificate-based advanced electronic signatures and qualified electronic signatures as defined in Article 3 (12) of the eIDAS Regulation. Hence, if said option is activated by the user, Adobe Sign can be considered as a business-friendly tool to support and facilitate the process of producing advanced and qualified electronic signatures.

In regard of the foregoing considerations, Adobe Sign, if configured accordingly, can be considered as a reliable electronic signature solution that allows one to manage an end-to-end signing process compliant with all types of electronic signatures available under the eIDAS Regulation. Adobe Sign in particular allows users to configure and build workflows in accordance with the user's specific compliance, industry and risk profile.

2 REGULATORY FRAMEWORK

2.1 eIDAS Regulation

eSign Directive – Until a few months ago, the use of electronic signatures in the EU was governed by Directive 1999/93/EC on a Community framework for electronic signatures (eSign Directive). The harmonisation brought about by that directive was imperfect and resulted in a lack of interoperability between electronic signature solutions in different EU member states and consequently lead to a fragmented market. Although the directive specified legal effects of electronic signatures, it did not

ensure that the recognition of an electronic signature in one EU member state also implied the acceptance of that same electronic signature in another EU member state. Hence, the acceptance of electronic signatures used in cross-border electronic transactions was highly uncertain. Moreover, the directive was no longer adapted to innovative solutions that also allow one to indicate that a person adopted the content of an electronic document or agreement.

To boost the use of electronic signatures and other trust services and to contribute to the creation of a digital single market across the EU, the European legislator adopted the eIDAS Regulation in July 2014. The eIDAS Regulation, of which most provisions only apply as from 1 July 2016, repealed the aforementioned directive on electronic signatures while building upon, clarifying and expanding the principles therein included.

eIDAS Regulation – Since the European legislature chose a regulation (that is directly applicable in all EU member states) instead of a revised directive (that would need to be transposed in the member states' national laws), businesses are no longer confronted with national electronic signatures laws but will only need to comply with one set of rules, significantly reducing the risk on interpretational issues. Although the eIDAS Regulation aims to ensure the legal effectiveness of electronic signatures and its admissibility as evidence in legal proceedings, just like its predecessor, it does not govern any aspects related to the conclusion and validity of (electronic) agreements (see section 2.2 below).

The eIDAS regulation makes a distinction between electronic signatures, advanced electronic signatures and qualified electronic signatures.

2.1.1 Standard electronic signatures

Broad definition – The eIDAS Regulation provides for a broad definition of a standard 'electronic signature' without any reference to a specific technology. Such standard 'electronic signature' is defined as data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

In its Recital 26, the eIDAS Regulation states that, because of the pace of technological change, an approach which is open to innovation should be adopted. Recital 27 further specifies that the eIDAS Regulation should be technology-neutral and that the legal effects it grants should be achievable by any technical means (provided that the requirements of the Regulation are met). The three criteria to qualify as a standard electronic signature are: (i) the existence of 'data in electronic form', (ii) 'attached to or logically associated with other data in electronic form' and (iii) 'used by the signatory to sign'. These criteria are not further defined or explained in the eIDAS Regulation and thus leave room for interpretation and technological innovation. In practice this means that many electronic tools that capture the intent of the signatory to approve the content of a document can be regarded as an electronic signature. This may amongst others be a PIN code, a password, a scanned signature, a symmetric or public key cryptography signature and a biometric signature.

Legal effect – According to Article 25.1 of the eIDAS Regulation, a standard electronic signature may not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures. Although the EU member states remain free to define the legal effects of standard electronic signatures, the effect of Article 25.1 is that they are not allowed to draft or maintain legislation nor to

endorse or authorise national rules with a view to reject the use of electronic signing tools solely because of their electronic format or non-qualified nature.

The fact that a standard electronic signature may not be denied legal effect and admissibility as evidence based on certain technical characteristics however does not mean that it would receive the same legal treatment as a handwritten signature. That will only be the case if set out in specific laws. Neither does it affect national rules regarding the free consideration of evidence by courts.

A standard electronic signature may not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that is in an electronic form and does not meet the requirements for qualified electronic signatures.

2.1.2 Advanced electronic signatures

Four criteria – An 'advanced electronic signature' is defined by Article 3 (10) of the eIDAS Regulation as a standard electronic signature that meets the requirements of Article 26 of the eIDAS Regulation, notably: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Although the legal definition of an advanced electronic signature has been formulated in a technology-neutral way, until today, the generally accepted interpretation has been that the concept mainly refers to electronic signatures that are based on digital signature technology or, in other words, that make use of public key cryptography. Within this interpretation, an advanced electronic signature must be seen as a digital file containing a hash of the document obtained by encryption with the private key of the signatory. The advanced electronic signature can consequently be verified with the corresponding public key of the signatory. A corresponding digital certificate, notably an electronic attestation which links the data for validating the signature to a natural person and confirms at least the name or the pseudonym of that person, confirms the signatory as the owner of his public key.

Remote signatures – The technology-neutral definition of advanced electronic signature however does not exclude that any other technologies would allow one to produce advanced electronic signatures, provided of course that the four aforementioned requirements are met. On the one hand, the Recitals 26 and 27 confirm that the eIDAS Regulation is or should be open to innovation and that the legal effects it grants should be achievable by any technical means. On the other hand, Recital 52 paves the way for the use of cloud-based electronic signature solutions in a legally effective way. That recital recognises that the creation of remote electronic signatures through an electronic signature environment managed by a trust service provider on behalf of the signatory is set to increase. Furthermore, it specifies in that respect that such electronic signatures should receive the same legal recognition as electronic signatures created in an entirely user-managed environment, provided that the remote electronic signature service provider applies specific management and administrative security procedures and uses trustworthy systems and products in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the

signatory. Given the broad formulation of this recital, it can be argued that a signatory can store his private key in the cloud or could even use a cloud-based electronic signature solution that does not require any signatory keys.

The eIDAS Regulation does not confer to the advanced electronic signature any specific legal effects that are different from a standard electronic signature. The concept is however used as a building block for defining the qualified electronic signature, which is an advanced electronic signature that satisfies a number of additional legal requirements (see section 2.1.3 below).

Increased level of trust – The main difference between standard electronic signatures and advanced electronic signatures however is that the technical security of an advanced electronic signature (often a digital certificate-based electronic signature) is generally considered to be higher than certain legally accepted standard electronic signatures, such as a PIN code or a scanned signature attached to a document. In general, advanced electronic signatures are thus considered to be more trustworthy and generally confer more evidential weight in court. However, from a legal perspective, the technical method used can only be one element to be taken into account at the discretion of the courts. Hence, in one particular case, the trustworthiness of a specific digital certificate-based electronic signature may be questioned, while in another case, a court may consider a PIN code to provide sufficient evidence.

Although no specific legal effects are attributed to an advanced electronic signature, it is generally considered to be more trustworthy and confer more evidential weight in court. Moreover, the eIDAS Regulation seems to leave room for electronic signatures that are not based on a digital certificate to qualify as an advanced electronic signature.

2.1.3 Qualified electronic signatures

Equal to handwritten signature – A 'qualified electronic signature' is defined by Article 3 (12) of the eIDAS Regulation as an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

A key principle of the eIDAS Regulation is that in accordance with its Article 25.2 a qualified electronic signature is automatically equivalent to a handwritten signature and has the equivalent legal effects. Article 25.3 further states that a qualified electronic signature based on a qualified certificate issued in one EU member state shall be recognised as a qualified electronic signature in all other EU member states. As such, Article 25.3 overcomes the lack of interoperability that plagued Directive 1999/93/EC on electronic signatures and enables secure and seamless cross-border electronic transactions by increasing the legal recognition of qualified electronic signatures across EU member states.

Extensive set of criteria – To be considered a qualified electronic signature, the electronic signature must be based on a qualified certificate. A 'qualified' certificate is a digital certificate which must contain the specific information set out in Annex I to the eIDAS Regulation and be issued by a qualified trust service provider (after having verified the identity and specific attributes, if any, of the

concerned natural person). A qualified trust service provider is a trust service provider who provides qualified trust services in accordance with the requirements set out in section 3 of the eIDAS Regulation. In practice, for qualified electronic signatures this means the commercial or governmental certificate authority that certifies the ownership of a named person's public key by issuing a digital certificate.

A qualified electronic signature must also be created by a qualified electronic signature creation device. This means that the configured software or hardware (e.g. a smart card, a USB token or a cloud-based hardware security module) used to create said signature must comply with the requirements relating to the trustworthiness of the data handled by the device as set out in Annex II to the eIDAS Regulation.

A qualified electronic signature automatically has the equivalent legal effect of a handwritten signature and must be recognised in other EU member states.

2.2 Validity and enforceability of electronic agreements

When considering the use of electronic signatures in the context of contractual agreements, assessing the legal effectiveness of the electronic signature is only one question to be addressed. Two other equally important questions arise. The first one relates to the validity of an electronically signed agreement. The second one relates to the evidentiary value and enforceability of an electronically signed agreement.

Validity – The first question that needs to be answered relates to the formal requirements to be fulfilled in order to validly conclude an agreement. Within European contract law 'consensualism' is a key principle. This means that the freely given and mutual consent of the contracting parties suffices to conclude a valid agreement and that no formal requirements, such as a written document, registration or signatures, are required.

Agreements can be entered into verbally, in writing, electronically or even implicitly. Exceptions to this general principle however exist in various EU member states. Real estate agreements, public procurement agreements, consumer agreements, settlement agreements, agreements of suretyship may require specific formalities to be fulfilled in order to conclude a valid agreement. While exceptions indeed exist, for the vast majority of agreements the mere consent of the contracting parties will suffice and no signatures will be needed to conclude a valid agreement.

Enforceability – The second question that needs to be answered relates to the way in which agreements can be validly enforced. From a legal perspective, this second question is highly relevant as there is a significant difference between concluding a valid agreement and also being able to enforce said agreement by proving its existence and contents.

The legal rules governing the evidentiary value and enforceability of agreements vary by jurisdiction. In civil law countries, such as Belgium, France and Italy, which may be seen as an example for the

rules on evidence in continental Europe, a distinction is made between free and regulated evidence. In B2B disputes, any form of evidence (e.g. any type of writing, testimony, e-mail or factual element) is admissible. It of course remains up to the court to evaluate the evidentiary value of the submitted evidence. In B2C disputes and in disputes between private persons the forms of evidence are regulated, meaning i.e. that if a dispute is valued above a certain amount, a signed agreement (this is a written document signed by the parties undertaking obligations) is typically required to enforce it.

In most jurisdictions it however is acceptable to contractually deviate from the rules of evidence. This means that contracting parties can agree which means of proof suffice, and/or which evidentiary value is attributed to certain documents. A typical example can be found in the terms and conditions of online banking services, which will often require the user to agree that confirming a transaction with a card reader shall be considered as an electronic signature meeting the functional requirements of a handwritten signature.

Furthermore, it must be emphasised that even when regulated evidence is legally required (such as a signed agreement), the rules of evidence will generally attribute some legal evidentiary value to free evidence (e.g. e-mails describing the content of the agreement), whether as a legal rule or in practice.

Although differences exist between EU member states, it is reasonable to state (i) that the vast majority of agreements do not require any formalities to be valid and (ii) that for the majority of contractual disputes any evidence (e.g. any type of electronic signature) is admissible when demonstrating the enforceability of an agreement.

3 COMPLIANCE ASSESSMENT OF ADOBE SIGN

3.1 Description of Adobe Sign

Cloud solution – Adobe Sign is a SaaS-based electronic signature solution that allows users to flexibly manage the document signature process. Adobe Sign handles all aspects of the electronic signature process, from providing user validation options to embedding the approval into the final document and sealing the document with a tamper-evident certification. At each step of the process, Adobe Sign handles user verification and links all the audit information from the signatory to his or her signature in the document. Adobe Sign can be used through Adobe Acrobat desktop software, a web browser, a mobile device or through APIs that connect to the user's existing business applications.

Signature process – To send a document for signature, the user uploads the document to Adobe Sign. Adobe Sign supports multiple source document formats that can be signed electronically. Users can specify one or more parties that need to sign the document, provide a message to the participants and optionally apply additional security controls to the document. Adobe Sign also enables users to

manually create form fields and signature locations in a document through a simple drag-and-drop web interface. Signatories will be required to fill in the necessary fields and sign at the appropriate locations during the signature process.

Authentication – Adobe Sign supports a range of options for verifying the identity of the Adobe Sign users and of the signatories.

Users of Adobe Sign authenticate themselves based on a unique user identifier that is either created by the user or assigned via an administrator (in case of enterprise accounts). Users can log in and authenticate themselves through the following types of user identifiers:

- Adobe Sign ID – Users use a verified e-mail address and password combination to securely log in to their account. Account administrators in an organisation can place additional requirements on the user's password (e.g. a minimum complexity and number of characters).
- Adobe ID – Users can use an Adobe ID to log in to Adobe Sign. An Adobe ID is an identifier that is used by all Adobe services for enabling access to those services. Organisations have flexibility in controlling whether their users can use an Adobe ID to log in to Adobe Sign.
- Google Gmail and Google Apps – Adobe Sign also supports user login via a Google Gmail or Google Apps account. Account administrators can control whether users can employ this method.
- Single sign-on (SSO) using Security Assertion Markup Language (SAML) – Enterprises seeking a tighter access control mechanism can enable SAML SSO to centrally manage their users through the corporate identity system. It enables account administrators to enforce strong access controls and ensure password requirements are aligned with the corporate information security policies.

Furthermore, Adobe Sign supports several options for the identification of a signatory – who is not necessarily an Adobe Sign user and is not required to first register with Adobe Sign – to be verified before signing a document.

Basic authentication is achieved by sending an e-mail with a unique URL to a signatory. Because most signatories have unique access to one e-mail account, this is considered the first level of authentication. The URL link required to sign the document is comprised of unique identifiers that are specific to the transaction and can be password protected by the Adobe Sign user. After having clicked on said URL link, signatories can use a mouse or pre-defined font styles to create a 'handwritten' signature on screen, upload an existing file (e.g. a scanned signature) or type in their name and click a button (displaying "*click to sign*") to sign.

In addition, Adobe Sign provides multi-factor authentication and offers other authentication mechanisms to establish the identity of the signatory, including unique passwords for individual signatories, phone authentication (voice or SMS) or social identity using the signatory's Facebook or Google account.

Document certification – After the signatories have signed the document, Adobe Sign certifies the document so that any changes to it will be evident. Adobe Sign implements its own PKI, which is compliant with the *Adobe Approved Trust List (AATL)* program that supports document certification. Adobe Sign automatically certifies a final PDF of the signed document before distributing it to all participants. When recipients download and open the signed filed in Adobe Acrobat or Adobe Reader, a blue banner is displayed at the top of the document, which certifies that no unauthorised source tampered with the document during transit or at any point since the certification was applied.

After all signatories have signed the document, Adobe Sign also automatically stores all signed documents in a centralised, secure repository where they are easily accessible, but users can choose to integrate the services into their existing document management solutions.

Audit trail – Adobe Sign allows real-time visibility into the signature process. Once the document has been sent out for signature, Adobe Sign automatically handles the workflow, monitoring, tracking, reminders and authentication to make the electronic signature process simple and easy.

Each key step in the signature process is logged, such as when the document was sent, opened and signed, IP addresses or geolocations of signatories and the specific form of authentication used for each signer or approver. The result is captured in a secured audit trail that provides, clear, easily producible evidence of each signatory's signature. The audit trail report can be retrieved by the Adobe Sign user through the Adobe Sign dashboard or by a signatory (that is not a user) by clicking on a signature in the signed document and entering the unique transaction ID to obtain access to the audit report.

Digital signatures – Adobe Sign does not only allow the creation of electronic signatures that are not based on a digital certificate but also supports the use of digital certificate-based signatures by using Adobe Sign in combination with Adobe Acrobat or Adobe Reader to capture digital signatures on documents. During the signing process, the signatory's certificate is cryptographically bound to the document using the private key held by that signatory. During the validation process, the reciprocal public key is extracted from the signature and used to both authenticate the signatory's identity and help ensure that no changes were made to the document since it was signed. In this regard, the audit trail also provides for additional, valuable information such as the signatory's IP address or geolocation.

Adobe is not a certificate authority. As a result, Adobe Sign does not issue digital certificates itself but works with virtually every digital certificate issued by third party trust service providers, many of which are recognised by Adobe Sign through the *Adobe Approved Trust List* (e.g. this list includes trust service providers such as DigiCert, GlobalSign, QuoVadis, etc.).

Cloud security – Adobe has put in place a number of technical and organisational measures related to physical data centre security, disaster recovery, environmental controls, logical security, data protection, intrusion detection, response and monitoring, to ensure the security of Adobe Sign and any related processes. Adobe Sign business processes are certified compliant with ISO 270001, SSAE SOC 2 Type 2 and PCI DSS.

Subscription plans – Adobe Sign can be used through three different subscriptions plans: 'individual', 'business' and 'enterprise'. Depending on the chosen subscription plan, Adobe Sign offers additional features. In particular, the multi-factor authentication is only available for the 'business' and 'enterprise' subscription plans, whereas the use of digital certificate-based electronic signatures is only available for the 'enterprise' subscription plan.

3.2 How Adobe Sign can support eIDAS compliance

This section of the white paper will review how the legal requirements for standard, advanced and qualified electronic signatures as set out above apply to Adobe Sign.

3.2.1 Adobe Sign meets the European requirements of standard electronic signatures

Requirements – In accordance with the definition of standard "electronic signatures" in the eIDAS Regulation, data in electronic form must be attached to or logically associated with other data in electronic form and be used by the signatory to sign.

Adobe Sign – In regard of the description of Adobe Sign as set out above, we conclude with confidence that from a legal point of view, Adobe Sign meets or even exceeds the requirements of standard electronic signatures:

- *'data in electronic form'* – Electronic signatures created with Adobe Sign indeed consist of a string of data in electronic form.
- *'attached to or logically associated with other electronic data'* – The electronic signature can be attached by the signatory to a variety of electronic documents, whereby Adobe Signs allow uploading multiple source document formats.
- *'used by the signatory to sign'* – Adobe Sign has been designed in such a way that there is a clear focus on capturing the intent of the signatory to sign in the signature process:
  - The signatory will receive an e-mail entitled "*Please sign* [Name of the document]*"* in which the hyperlink to Adobe Sign states the following: "*Click here to review and sign* [Name of the document]*";*
  - When the signatory reviews the document, he is requested to sign the document by typing his name, creating a 'handwritten' signature on screen or by uploading an image of a scanned signature. The signatory is prompted to do so by a form field in the document that mentions "C*lick here to sign*".;
  - After this has been done, a notice appears that states "*I agree to the Terms of Use and Consumer Disclosure of this document"* together with a button "*click to sign*". Only once the signatory clicks this button and confirms a second time his intent to sign, does Adobe Sign consider the document signed and circulates it to the other participants.

  Although the appearance of the signature on the document can be seen only as a visual, esthetical feature without impact on the value of the electronic signature, the multi-faceted approach to capturing the intent of the signatory to sign allows to meet this third criterion. This is not only a requirement to produce standard electronic signatures but also an important aspect in contract formation. As agreements, as a principle, are entered into by the mutual consent of the contracting parties, having a clear signature process helps in demonstrating the willingness of the signatory to be bound by legal obligations and deducing consent.

This means, according to Article 25.1 of the eIDAS Regulation, that an electronic signature produced with Adobe Sign, may, in principle, not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds of its technical features. This however does not mean that such an

electronic signature automatically acquires the same legal validity as a handwritten signature, unless of course a qualified certificate is used (see section 3.2.3 below).

Moreover, Adobe Sign offers a number of features that could strengthen the enforceability as an electronic signature, compared to other commonly accepted electronic signatures, such as:

- The audit trail – If the validity of the electronic signature were challenged, the audit trail that is generated by Adobe Sign could serve as relevant proof to demonstrate the link between the identity of a signatory and a signature.
- The multi-factor authentication methods – If multi-factor authentication were required from the signatory, by selecting the appropriate settings, this inevitably increases the ability to properly authenticate the signatory and produce electronic signatures with an increased evidentiary value.

It follows from the foregoing that Adobe Sign is not a merely a solution that allows one to produce standard electronic signatures in compliance with the eIDAS Regulation: it can be considered that Adobe Sign is a trustworthy and secure way to do so.

Adobe Sign allows one to produce standard electronic signatures in a trustworthy and secure way. Adobe Sign (i) permits one to identify the signatories in an advanced way, (ii) captures the intent to sign in an unambiguous way and (iii) manages an audit trail record to support the enforcement of the produced electronic signature.

3.2.2 Adobe Sign and advanced electronic signatures

Requirements – In accordance with the definition of advanced electronic signatures in the eIDAS Regulation, such an electronic signature must be uniquely linked to the signatory, capable of identifying the signatory, created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control and be linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Adobe Sign – In regard of the description of Adobe Sign as set out above, we conclude with confidence that from a legal point of view, Adobe Sign supports the production of digital certificate-based advanced electronic signatures.

As set out above, the requirements of advanced electronic signatures are typically met by digital certificate-based electronic signatures and Adobe does not issue and manage certificates to produce such signatures. Adobe Sign however contains a native integration with Adobe Acrobat and Adobe Reader to enable the creation of so-called ‘digital signatures’. For the avoidance of doubt, it must be emphasised that the concept of ‘digital signature’, as used by Adobe Sign, is not legally defined in the eIDAS Regulation, but must be interpreted as including digital certificate-based advanced electronic signatures, qualified electronic signatures as well as electronic signatures based on self-signed certificates.

If a document is uploaded to Adobe Sign for signature, the Adobe Sign user can require the signatories to use a digital signature by adding a digital signature form field to the document. The signatories will then be prompted to download the document, which will open in Adobe Acrobat or Adobe Reader (depending on what is installed on the signatory's computer) and then the signatory will be guided to the signature field and will be able to select a certificate on his device and apply the advanced electronic signature to the document in Adobe Acrobat or Adobe Reader. The signed document will then automatically be uploaded to Adobe Sign (without any additional specific signatory action being required), the other signatories will be notified and a record of the digital signature is captured within the audit trail for the document. Although the audit trail will only mention that the document has been signed digitally, the validity of the digital certificate that has been used, can be verified by the Adobe sign user and the signatories by consulting the signed document itself via Adobe Sign or by opening the document directly in Adobe Reader or Adobe Acrobat.

Digital certificate-based advanced electronic signatures can be integrated in an end-to-end electronic signature process that is supported by and managed through Adobe Sign.

As set out in section 2.1.2 above, there are arguments to state that signature technologies other than public key cryptography, such as for example process-focused cloud-based electronic signature solutions may be able to meet the requirements of advanced electronic signatures. Hence, if Adobe Sign's 'digital signatures' feature is disregarded and the solution is assessed in regard of the four criteria of an advanced electronic signature, the following must be observed:

- *'uniquely linked to the signatory'* – Adobe Sign allows one to link every electronic signature that is produced on the platform to a signatory. Adobe Sign offers multi-factor authentication methods to clearly authenticate signatories. In addition, the audit trail that keeps track of all electronic signatures in a document allows one to link a specific signature to a specific signatory.
- *'capable of identifying the signatory'* – To ensure this requirement is met, users are advised to require multi-factor authentication to log in to and sign the document, instead of merely requiring one to click on a hyperlink to obtain access.
- *'created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control'* – Typically only digital certificate-based advanced electronic signatures are considered as being able to meet this criterion, whereby the private key of the signatory is seen as the 'electronic signature creation data'. The concept of 'electronic signature creation data' is however not necessarily limited to private keys, as the eIDAS Regulation defines it in a broad way as 'unique data which is used by the signatory to create an electronic signature'.

  In regard of Recital 52 of the eIDAS Regulation, also cloud-based electronic signature solutions (that are not necessarily based on digital certificates) may be able to meet this criterion provided that specific management and security procedures are put in place and trustworthy systems and products are used to guarantee that the electronic signature creation environment is reliable and under the sole control of the signatory. When use is made of strong multi-factor authentication methods to get access to the personalised signing environment and to the to be signed document

itself, it may be argued that the Adobe Sign platform indeed allows one to create electronic signatures with means that are with a high level of confidence under the control of the signatory. Relevant to emphasise in this regard is that Adobe administrators themselves do not have access to any user accounts or signatory profiles nor to any log-in details (including passwords) to obtain access to such accounts or profiles

- *'linked to the data signed therewith in such a way that any subsequent change in the data is detectable'* – After the signatories have signed the document, Adobe Sign automatically certifies the signed document with its digital certificate to protect the document against any subsequent changes. Moreover, once a document is signed with Adobe Sign any subsequent change becomes easily visible as the audit trail records all activities and changes with regard to the concerned document.

Although arguments exist to state that Adobe Sign allows to produce advanced electronic signatures that are not based on a digital certificate, it must be stressed that such arguments have not been tested in court. Nevertheless, users should at all times keep in mind that the eIDAS Regulation does not confer to the advanced electronic signature any specific legal effects that are different from a standard electronic signature. Hence, even if a court would decide that Adobe Sign, without making use of digital certificates, does not allow to produce advanced electronic signatures, that does not mean that the trustworthiness and reliability of Adobe Sign would decrease. In any event, as set out above, Adobe Sign should be seen as a trustworthy and secure tool to use for electronic signature processes.

Arguments exist to state that Adobe Sign allows one to produce advanced electronic signatures that are not based on a digital certificate.

3.2.3 Adobe Sign and qualified electronic signatures

Requirements – In accordance with the eIDAS Regulation, a qualified electronic signature is legally equivalent to a handwritten signature and shall be recognised as such in all other EU member states. A set out above, the eIDAS Regulation defines a qualified electronic signature as an advanced electronic signature with the additional requirements that it must be based on a qualified certificate and created by a qualified electronic signature creation device.

The first requirement is the use of a qualified certificate. This means a digital certificate that is issued by a qualified trust service provider and meeting the requirements of Annex I to the eIDAS Regulation. In regard of the requirements of the eIDAS Regulation, a certificate containing a signatory key and the identity of the owner issued by a qualified commercial or governmental certificate authority fulfils the definition of a qualified certificate.

The second requirement is the use of a qualified electronic signature creation device. Such a device is configured hardware or software (e.g. a smart card, a USB token or a cloud-based hardware security

module) used to create an electronic signature and meeting the requirements of Annex II to the eIDAS Regulation.

Adobe Sign – Adobe Sign does not manage or issue qualified certificates and does not offer qualified electronic signature creation devices, but, we conclude with confidence that from a legal point of view, Adobe Sign supports the production of qualified electronic signatures through its interoperation with qualified certificate providers.

Adobe Sign contains a native integration with Adobe Acrobat and Adobe Reader to enable so-called 'digital signatures'. For the avoidance of doubt, it must be emphasised that the concept of 'digital signature', as used by Adobe Sign, is not legally defined in the eIDAS Regulation, but must be interpreted as including digital certificate-based advanced electronic signatures, qualified electronic signatures as well as electronic signatures based on self-signed certificates.

If a document is uploaded to Adobe Sign for signature, the Adobe Sign user can require the signatories to use a digital signature by adding a digital signature form field to the document. The signatories will then be prompted to download the document, which will open in Adobe Acrobat or Adobe Reader (depending on what is installed on the signatory's computer) and then the signatory will be guided to the signature field and will be able to select a certificate on his device and apply the qualified electronic signature to the document in Adobe Acrobat or Adobe Reader. The signed document will then automatically be uploaded to Adobe Sign (without any additional specific signatory action being required), the other signatories will be notified and a record of the digital signature is captured within the audit trail for the document. Although the audit trail will only mention that the document has been signed digitally, the validity of the digital certificate that has been used, can be verified by the Adobe sign user and the signatories by consulting the signed document itself via Adobe Sign or by opening the document directly in Adobe Reader or Adobe Acrobat.

As in some cases the use of qualified electronic signatures is required to validly sign an agreement electronically, the Adobe Sign users and signatories are recommended to verify that the appropriate settings are activated in order to be able to conclude a valid agreement.

For the sake of completeness, it must be mentioned that Adobe Acrobat and Adobe Reader indeed have features to identify qualified certificates, by means of standard qualified certificate statements and on the basis of the EU Trusted List, to validate and trust qualified certificates based on the EU Trusted Lists, to identify qualified signature creation devices by means of standard qualified certificate statements and to support digital signatures in the PAdES Baseline format (both ETSI TS 103 172 and the newest ETSI EN 319 142-1).

Qualified electronic signatures can be integrated in an end-to-end electronic signature process that is supported by and managed through Adobe Sign.

4 CONCLUSION

Adobe Sign is a SaaS-based electronic signature solution that handles all aspects of the electronic signature process, from providing user validation options to embedding the approval into the final document and sealing the document with a tamper-evident certification.

Adobe Sign supports a range of options for verifying the identity of the Adobe Sign users and signatories, i.e. through the use of specific identifiers (e.g. Adobe (Sign) ID or Google Gmail account) and (multi-factor) authentication methods (e.g. unique passwords, phone authentication (voice or sms) or social identity). Moreover, the processes underpinning Adobe Sign have been designated in such a way that they clearly focus on capturing the intent of the signatories. Finally, to protect the signed document against any subsequent changes, Adobe Sign maintains an audit trail that registers any changes made to the signed document and certifies the final document before circulating it to all participants.

From a legal perspective, we can conclude with confidence that when the appropriate user settings are selected, Adobe Sign is a trustworthy and secure tool that allows to produce standard electronic signatures that meet or even exceed the requirements of a standard "electronic signature" as defined in Article 3 (10) of the eIDAS Regulation. This means that according to Article 25.2 of the eIDAS Regulation, they may not be denied legal effectiveness solely based on their technical characteristics. Although a standard electronic signature does not automatically have the same legal effect as a handwritten signature, from the perspective of the intended use of electronic signatures as a means to more easily and flexibly conclude valid agreements and from an enforceability point of view, standard electronic signature are often considered as adequate. When courts need to assess the value of the submitted evidence to the them, they will generally give more evidential weight to documents that are electronically signed with more trustworthy and secure technology. In this respect, Adobe Sign provides important evidentiary value by providing a multi-factor authentication, registering every single action on Adobe Sign and certifying the signed document.

Moreover, we believe that arguments exist to state that Adobe Sign, without the use of digital signature technology, may allow to produce "advanced electronic signatures" as defined in Article 3 (11) of the eIDAS Regulation. As the eIDAS Regulation does not attribute any specific legal effects to advanced electronic signatures other than to standard electronic signatures, it must be observed that even if the legal requirements of an advanced electronic signature would not be met, Adobe Sign still must be seen as a trustworthy and secure electronic signature solution.

Furthermore, we observe that Adobe Sign also contains an option supporting the use of digital signature technology, notably digital certificate-based advanced electronic signatures and "qualified electronic signatures" as defined in Article 3 (12) of the eIDAS Regulation. Hence, if said option is activated by the user, Adobe Sign can be considered as a business-friendly tool to support and facilitate the process of producing advanced and qualified electronic signatures. In the case of qualified electronic signatures, this means that Adobe Sign supports the creation of electronic signatures that, in accordance with Article 25 of the eIDAS Regulation, have the equivalent legal effect of a handwritten signature and are recognised in other EU member states.

Adobe Sign is a reliable electronic signature solution that allows one to manage an end-to-end signing process compliant with all types of electronic signatures available under the eIDAS Regulation. Adobe Sign in particular allows users to configure and build workflows in accordance with the user's specific compliance, industry and risk profile.

5 ABOUT THE AUTHOR

Prof. dr. Patrick Van Eecke is a partner in the IT law Department of DLA Piper in Brussels. Patrick is member of the Brussels bar and is associate member of the American Bar Association. Dr. Van Eecke advises both public administrations and enterprises on the legal compliant implementation of e-signature solutions and is experienced in drafting and negotiating PKI related legal documents, such as Certification Practice Statements, Certificate Policies, Signature Policies and Relying Party Agreements.

Patrick Van Eecke is extensively involved in diverse research and consulting projects for the European Commission and several national governments. For example, he was involved in the first European Commission Study on the legal aspects of electronic signatures (1998), the EC Study on electronic signature policies (2001), the EC Study on long term archiving of electronic signatures (2001) and EC Study on the legal and market aspects of electronic signatures (2003). He was the lead consultant in the EC study on the future of the ICT standardisation policy (2006). More recently, he was extensively involved in the European Commission Study Feasibility study on an electronic identification, authentication and signature policy (IAS) (2010) as well as in the EC Study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market (2014).

As a national representative, Patrick was involved in the European Council debates on the directive on electronic signatures and the directive on electronic commerce. He was also advising the Economic and Social Committee of the European Communities on these matters. As the legal expert of the EESSI expert team (European Electronic Signature Standardisation Initiative) he was co-author of the first EESSI report and following legal deliverables.

Dr. Van Eecke obtained his PhD at the University of Leuven (including a visiting scholarship at Stanford University) having as subject “The legal status of electronic signatures” (2003). He is a professor at the University of Antwerp, teaching European Information and Communications Law. He is also a guest lecturer at Kings College and Queen Mary University (London). Patrick is the author of several legal articles and books on computer crime, electronic signatures, electronic contracting and privacy and is a regular speaker on national and international conferences.

* *

*

www.dlapiper.com