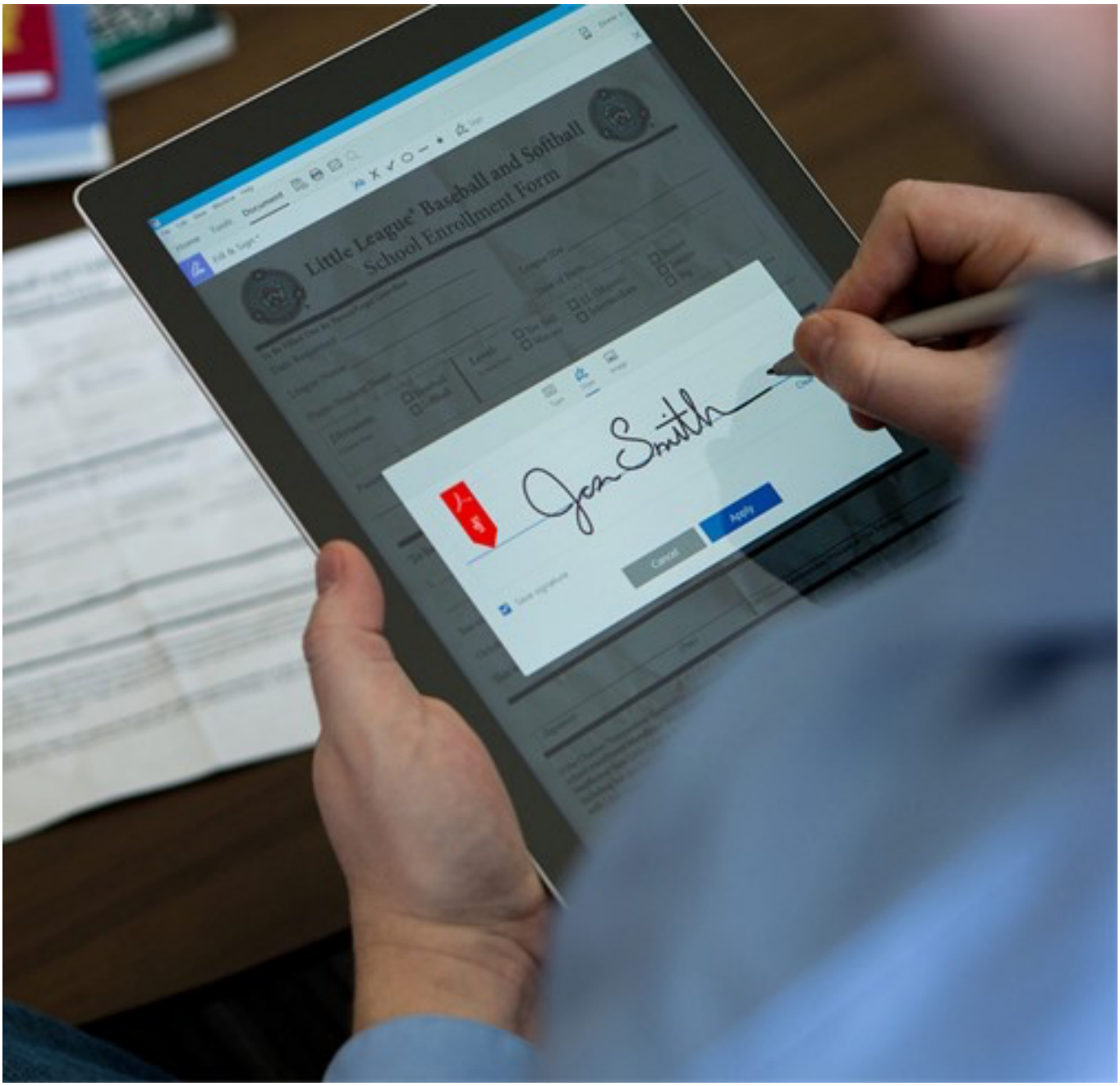

Adobe Acrobat Sign

COMPLIANCE WITH EUROPEAN AND UK ELECTRONIC SIGNATURE LEGISLATION

July 2024

Contents

1 INTRODUCTION....3

2 EU REGULATORY FRAMEWORK....4

2.1 eIDAS Regulation....4

(a) Standard electronic signatures....4

(b) Advanced electronic signatures....5

(c) Qualified electronic signatures....7

2.2 Validity and enforceability of electronic agreements....8

2.3 The mutual recognition of qualified electronic signatures....9

(a) Within the EU....9

(b) Post-Brexit in the UK....9

3 UK REGULATORY FRAMEWORK....11

3.1 UK eIDAS Regulation....11

3.2 Types of electronic signatures....11

(a) Simple electronic signatures....11

(b) Advanced electronic signatures....12

(c) Qualified electronic signatures....12

3.3 Validity and enforceability of electronic agreements in the UK....13

4 COMPLIANCE ASSESSMENT OF ADOBE ACROBAT SIGN....15

4.1 Description of Adobe Acrobat Sign....15

4.2 How Adobe Acrobat Sign can support compliance with the EU eIDAS and UK eIDAS Regulations....18

(a) Adobe Acrobat Sign meets the European and UK requirements of standard electronic signatures....19

(b) Adobe Acrobat Sign and advanced electronic signatures....20

(c) Adobe Acrobat Sign and qualified electronic signatures....22

5 CONCLUSION....24

1 Introduction

This white paper assesses the legal effectiveness of the Adobe Acrobat Sign solution in relation to European and UK requirements applicable to electronic signatures. In the first part of this white paper, we give an overview of the relevant legal framework for both the EU and the UK.

For the EU, 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 the **EU eIDAS Regulation**), which is the core instrument governing the validity of electronic signatures in the EU. We will further analyse key questions relating to the validity and enforceability of electronically signed agreements and the mutual recognition of electronic signatures.

For the UK, we briefly describe the scope, main concepts and legal consequences of the retained law version of Regulation (EU) 910/2014 the Electronic Identification and Trust Services for Electronic Transfers in the Internal Market (eIDAS) as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/89) and Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (2016 No.696) (hereafter the **UK eIDAS Regulation**), and how the UK eIDAS Regulation allowed for an amended version of the EU eIDAS Regulation to become enshrined in UK Law post-Brexit. We will go on to discuss the regulatory framework set out in the UK eIDAS Regulation and the implications this has for business, consumers and other users as the core instrument governing the validity of electronic signatures in the UK. We will further analyse key questions relating to the validity and enforceability of electronically signed agreements.

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

We conclude that when the appropriate user settings are selected, Adobe Acrobat 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 EU eIDAS Regulation and the UK eIDAS Regulation.

Furthermore, we observe that Adobe Acrobat Sign contains an option supporting the use of digital signature technology, notably advanced electronic signatures as defined in Article 3 (11) of the EU eIDAS/UK eIDAS Regulations, and qualified electronic signatures as defined in Article 3 (12) of the EU eIDAS/UK eIDAS Regulations. Hence, if said option, which enables the creation of digital signatures with both desktop and cloud-based deployments, is activated by the user, Adobe Acrobat Sign is an innovative and business-friendly tool to support and facilitate the process of producing advanced and qualified electronic signatures. Moreover, Adobe Acrobat Sign offers reliable means to guarantee the long-term validity of such electronic signatures through Adobe's own qualified electronic time stamp service, or alternatively via its integration with third party electronic time stamp services.

When properly configured, Adobe Acrobat 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 EU eIDAS and UK eIDAS Regulations. Adobe Acrobat Sign in particular allows users to configure and build workflows in accordance with the user's specific compliance, industry and risk profile.

2 EU regulatory framework

2.1 eIDAS Regulation

eSign Directive – Up until July 2016, 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 the eSign Directive was imperfect and resulted in a lack of interoperability between electronic signature solutions in different EU member states and resulted in a fragmented market. Although the eSign Directive specified the 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.

To boost the use of electronic signatures and other trust services (such as electronic time stamp services), and to contribute to the creation of a digital single market across the EU, the European legislators adopted the EU eIDAS Regulation in July 2014. The EU eIDAS Regulation repealed the eSign Directive on electronic signatures while building upon, clarifying and expanding its core principles. The majority of its provisions became law in July of 2016.

EU 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 disparate national electronic signatures laws but will only need to comply with one set of rules, significantly reducing the risk on interpretational issues. Although the EU 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 EU eIDAS Regulation makes a distinction between electronic signatures, advanced electronic signatures and qualified electronic signatures.

(a) Standard electronic signatures

Broad definition – The EU eIDAS Regulation provides for a broad definition of a standard 'electronic signature' without any reference to a specific technology. A 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 Recital 26, the EU eIDAS Regulation states that, because of the pace of technological change, an innovative approach should be adopted. Recital 27 further specifies that the EU 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 EU eIDAS 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 EU 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 include a PIN code, a password, a scanned signature, a symmetric or public key cryptography signature or a biometric signature.

Legal effect – According to Article 25.1 of the EU 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. This is known as the 'non-discrimination' principle. Although EU member states remain free to define the legal effects of standard electronic signatures, the effect of Article 25.1 is that they may not draft or maintain legislation, nor endorse or authorise national rules that exclude 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. Indeed, EU Member States remain free to define the legal effects of standard electronic signatures in specific national laws. Further, this provision does also not 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 it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

(b) Advanced electronic signatures

Four criteria – An 'advanced electronic signature' is defined by Article 3 (10) of the EU eIDAS Regulation as a standard electronic signature that meets the requirements of Article 26 of the EU 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.

Public-key cryptography – Although the legal definition of an advanced electronic signature has been formulated in a technology-neutral way, until today, a generally accepted interpretation is that these requirements are satisfied by electronic signatures that are based on digital signature technology that make use of public key cryptography. Within this interpretation, an advanced electronic signature must be seen as a digital file generated by encryption of the hash of the document with the private key of the signatory. The advanced electronic signature can consequently be verified with the corresponding public key of the signatory contained in the signing certificate. In this respect a digital certificate is typically issued by a trust service provider and, confirms at least the name or the pseudonym of the signatory, as well as the signatory as the owner of their 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 EU 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 likely to see increased usage. Furthermore, it specifies that such remote 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, a signatory could store his private key in the cloud or it could maybe even use a cloud-based electronic signature solution that does not require any signatory keys at all, as set out above, provided of course that the four aforementioned requirements are met.

Increased level of trust – The EU eIDAS Regulation does not confer on 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(c) below).

The main difference between standard electronic signatures and advanced electronic signatures is that the technical security of an advanced electronic signature is generally considered to be higher than 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, 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.

In addition, it should be noted that EU member states could require the use of advanced electronic signatures (instead of standard electronic signatures) in certain transactions. In our experience, however, where EU member states decide to require a specific type of electronic signature, this is often a qualified electronic signature, rather than an advanced electronic signature.

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 EU eIDAS Regulation paves the way for the use of cloud-based advanced

electronic signatures whereby the electronic signature environment is managed by a trust service provider on behalf of the signatory.

(c) Qualified electronic signatures

Extensive set of criteria – A 'qualified electronic signature' is defined by Article 3 (12) of the EU 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 'qualified' certificate is a digital certificate which must contain the specific information set out in Annex I to the EU 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 EU eIDAS Regulation and is granted qualified status by a national supervisory body. 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 (qualified) digital certificate.

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

Remote signatures – In addition to what is set out in the corresponding paragraph of the above section 3.2(b) on advanced electronic signatures, it must be emphasised that with regard to qualified electronic signatures, Recital 51 of the EU eIDAS Regulation confirms even more explicitly that one can entrust qualified electronic signature creation devices to the care of a third party (e.g. a cloud-based hardware security module (HSM)), provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data (e.g. the private key is controlled in an exclusive way by the owner when creating a qualified electronic signature). An example of sole control is using a mobile app with a one-time passcode or biometric authentication.

Equal to handwritten signature – A key principle of the EU eIDAS Regulation is that in accordance with Article 25.2, a qualified electronic signature is automatically deemed equal to a handwritten signature and has 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 and cross-recognition that hampered 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.

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 of the questions 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 generally be entered into verbally, in writing, electronically or even implicitly. Nevertheless, exceptions to this general principle exist in many EU member states. For example, real estate agreements, public procurement agreements, consumer agreements, settlement agreements and agreements of suretyship may require specific formalities 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. Of course, the use of a signature is helpful in recording and evidencing a party's consent to an agreement.

Enforceability – The second question that needs to be answered relates to the way in which agreements can be validly enforced. This second question is highly relevant as there is a significant difference between concluding a valid agreement and being able to enforce that 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 exemplify 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 this context, article 25.1 of the EU eIDAS Regulation provides that electronic signatures shall 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. Thus, electronic signatures can be used as evidence, but their evidential weight will depend on the type of electronic signature that is being used, whereby a qualified electronic signature or advanced electronic signature will typically have a higher probative value than a standard electronic signature.

However, in most jurisdictions it is acceptable to contractually deviate from the rules of evidence. This means that contracting parties can agree which means of proof will 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.

2.3 The mutual recognition of qualified electronic signatures

(a) Within the EU

Mutual recognition – According to Articles 25 and 35 of the EU eIDAS Regulation, qualified electronic signatures (and seals) which are based on qualified certificates issued in one member state, shall be recognised as a qualified signature (or seal) in other member states.

It should be noted that, according to Article 14 of the EU eIDAS Regulation, it is also possible for third countries (i.e. non-member states) to align their trust scheme with the European one and by doing so, ultimately reach a mutual recognition of qualified trust schemes.

Qualified electronic signatures based on qualified certificates issued in one EU member state, shall be recognised as a qualified signature in other EU member states. It is also possible for third countries (i.e. non-EU member states) to align their trust scheme with the European one and by doing so, ultimately reach a mutual recognition of qualified trust schemes.

(b) Post-Brexit in the UK

UK qualified electronic signatures – As a consequence of the UK's Brexit, the UK was removed from the EU's mutual recognition and interoperability framework under the EU eIDAS Regulation, and UK registered qualified trust service providers were no longer recognised in the EU bloc. This means that qualified certificates for signatures or seals no longer carry qualified status in the EU. The UK is also no longer obliged to notify the European Commission of its list of qualified trust service providers, and under the Data Protection and Digital Information Bill currently before Parliament, the UK government will, when the new law comes into force, publish a document setting out rules concerning the provision of digital verification services (to be known as the "DVS Trust Framework") and there will be a new public register of digital verification services (the "**DVS Register**"). The DVS Trust Framework will over time set different rules for different digital verification services, set different conditions for approval or designation for different purposes, and specify different commencement times for different purposes. The Bill also makes provision for the Secretary of State to publish a supplementary code with supplementary rules to those within the DVS Trust Framework, recognising that this is an evolving sector.

EU qualified electronic signatures –The relationship between the EU and UK regarding qualified electronic signatures and qualified trust service providers, is asymmetric in nature. Whilst UK qualified trust service providers have lost access to the EU market, EU entities' ability to access the UK market has remained unchanged. The UK eIDAS Regulation was designed to ensure the technical standards and specifications in the UK's domestic law mirrored those within the EU. Therefore, notwithstanding the UK's loss of access to the EU eIDAS interoperability network, the UK's legislative framework allows for EU trust services to remain valid for use in the UK. Therefore, there is no distinction in UK law between the validity of domestic and EU qualified electronic signatures. The UK's recognition of qualified trust service providers operating under the EU eIDAS Regulation means that a qualified electronic signature created using an EU issued qualified certificate has the same legal standing as a qualified electronic signature created using a domestic qualified trust service provider registered in the UK.

Practical implications – Ultimately, Brexit and the implementation of the UK eIDAS Regulation has had no impact on the manner in which EU-based qualified trust service providers can operate within the UK. The UK has preserved the principles of mutual recognition and interoperability for EU trust service providers. For avoidance of doubt, this includes all trust services including electronic seals, electronic signatures, electronic time stamps, electronic registered delivery and website authentication. Hence, EU trust service providers have experienced no change to the regulatory framework for their operations within the UK.

Any organisation wishing to offer trust services in the EU (rather than the UK), will need to comply with the EU eIDAS Regulation, including operating under the supervision of a supervisory body from another EU member state.

If the Data Protection and Digital Information Bill is enacted in its current form, when it comes into force it will change the regulatory landscape for digital verification services within the UK. Qualified trust service providers shall be required to register on the DVS Register and may be subject to a statutory code under the DVS Trust Framework, however there is no timescale currently when the DVS Trust Framework will be in force, and it is therefore not possible to comment on what regulatory requirements may apply. It is likely to mean however that qualified trust service providers will be subject to parallel regulatory regimes, and if they operate in both the UK and EU, will be required to register under both.

As a consequence of the UK's Brexit, the UK was removed from the EU's mutual recognition and interoperability framework and UK registered qualified trust service providers lost their recognition. The exclusion from the EU's internal framework has therefore removed UK qualified trust service providers' ability to provide automatically recognised qualified trust services in the EU. The UK has however preserved the principles of mutual recognition and interoperability for EU trust service providers in the UK, so EU trust service providers' qualified trust services are recognized in the UK.

3 UK regulatory framework

3.1 UK eIDAS Regulation

Prior to the UK's withdrawal from the EU, the legal framework in in relation to electronic signatures was aligned to that of the European Union. Regulation (EU) 910/2014 (the Electronic Identification and Trust Services for Electronic Transfers in the Internal Market Regulation (**EU eIDAS Regulation**) constituted the legal basis for the use of qualified trust services providers and qualified electronic signatures within the UK. Following Brexit, as with other aspects of EU laws, the UK Government took steps to ensure continuity by enacting domestic regulations that mirror the original EU regulation with amendments as deemed appropriate.

Accordingly, the EU eIDAS Regulation was incorporated into UK Law by section 3 of *the European Union (Withdrawal) Act 2018* (EUWA), to form part of the new body of retained EU law created by the EUWA and subsequently amended by the *Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019* (SI 2019/89) (the "**UK eIDAS Regulation**").

The UK eIDAS Regulation is an amended form of the EU eIDAS Regulation. The EU eIDAS Regulation provisions on electronic identification and notified e-ID schemes have been repealed. Other provisions relating to trust services (notably electronic signatures) have been retained with minor amendments. Although the UK eIDAS Regulation preserves the legal standing of EU qualified trust service providers in the UK, there is no reciprocity for UK qualified trust service providers in EU member states.

The UK eIDAS Regulation therefore does not include the provisions relating to electronic identification schemes and excludes Chapter II of the EU eIDAS Regulation. Chapter II was deemed to be redundant due to the removal of the UK's access to the EU's interoperability framework for e-ID. This removal of access was a consequence of the UK's post-Brexit third country status regarding the implementation and application of EU law in Member States. The UK's new status meant that EU Member States would no longer recognise the UK's national e-ID scheme, and vice versa. Moreover, when the UK Digital Information and Attributes Trust Framework (**UK DIATF**) comes into force in 2024, it will not be recognised as the UK's e-ID scheme under the EU eIDAS Regulation.

3.2 Types of electronic signatures

The UK eIDAS Regulation makes a distinction between simple electronic signatures, advanced electronic signatures and qualified electronic signatures in the same manner as the EU eIDAS Regulation.

(a) Simple electronic signatures

Criteria – Simple electronic signatures are the most basic form of electronic signature. It is defined, at Article 3(10) of the UK eIDAS Regulation as: "*data in electronic form which is attached to or logically associated with other date in electronic form and which is used by the signatory to sign.*" This definition is mirrored in section 7 of the Electronic Communications Act too. Examples of simple electronic signatures include an electronic signature made using a commercial e-signing platform or typing a signatory's name into an electronic document. Therefore, the level of reliance that contracting parties can place on a simple electronic signature is very much dependent on the context and type of contractual agreement. It is useful for everyday low risk transactions where the parties are comfortable in accepting a lower evidential standard in exchange for ease and speed of process.

Validity – Article 25(1) of UK eIDAS Regulation confirms that: an electronic signature shall 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. Whilst agreements executed by simple electronic signatures are generally accepted for most commercial transactions in the UK, questions may arise as to their enforceability down the line. This is largely down to the fact that – save where the parties use an e-signing platform - simple electronic signatures do not specifically demonstrate the intention of the signatory to authenticate the document (**authenticating intention**). Hence, in the absence of a reliable audit trail, it might be argued that there is a lack of evidence to show that the signatory possessed an authenticating intention.

A simple 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.

(b) Advanced electronic signatures

Criteria – An advanced electronic signature is defined by Article 3 (10) of the UK eIDAS Regulation as a standard electronic signature that meets the requirements of Article 26 of the UK eIDAS Regulation, being: (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.

Validity – As addressed earlier, electronic signatures are a valid form of execution of documents under UK Law. There is generally no distinction drawn between the validity of a simple electronic signature and an advanced electronic signature. However, an advanced electronic signature does provide additional assurance to the signatory that is not afforded by a simple electronic signature. The requirements around identity verification and cryptographic security imposed by Article 26 therefore, generally, give advanced electronic signatures more evidentiary weight if a court were required to consider the signed document in legal proceedings.

Although no specific legal effects are attributed to an advanced electronic signature in comparison to a simple electronic signature, it is generally considered to be more trustworthy and confer more evidential weight in court.

(c) Qualified electronic signatures

Criteria – Qualified electronic signatures are the most complex and are regarded as the gold standard of electronic execution. Qualified electronic signatures require that a qualified trust service provider verify the identity of the signatory before they are issued with the means to create the qualified electronic signature. In addition to having the same requirements as an

advanced electronic signature, a qualified electronic signature must be created using a qualified electronic signature creation device which is based on a qualified certificate for electronic signatures. Annex II of the UK eIDAS Regulation outlines the necessary technical and security requirements that must be fulfilled by qualified signature creation devices. As per the UK eIDAS Regulation, the cryptographic keys used for electronic signature creation must: (i) be kept confidential; (ii) only be used for the creation of the relevant electronic signature once; (iii) reliably be protected against forgery using currently available technology; and (iv) reliably protected by the legitimate signatory against use by others. In addition to the requirements outlined in Annex II, qualified electronic signature creation devices must also be certified by an approved conformity assessment body and abide by the UK eIDAS Regulation (Article 30 security assessment standards).

Validity – The validity of a qualified electronic signature is confirmed by adhering to validation criteria set out in Article 32 of the UK eIDAS Regulation. Article 32 requires that: (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I; (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing; (c) the signature validation data (i.e. public cryptographic key) corresponds to the data provided to the relying party; (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing; (f) the electronic signature was created by a qualified electronic signature creation device; (g) the integrity of the signed data has not been compromised; and (h) the requirements provided for in Article 26 were met at the time of signing (being the requirements as previously noted for advanced electronic signatures).

Qualified electronic signatures are the most complex and have the highest standard of electronic subscription. The validity of a qualified electronic signature is confirmed by abiding by the Article 32 validation criteria.

3.3 Validity and enforceability of electronic agreements in the UK

Validity – The first question that needs to be answered concerns the formal requirements to be fulfilled in order to validly conclude an agreement.

For the majority of transactions in the UK, the common law does not prescribe a particular form or type of signature for execution. This is largely due to the fact that there is no general prescribed method for entering into a contractual agreement under common law. The UK eIDAS Regulation provides legal recognition to all forms of electronic signatures. As such, where: (a) signatory has the necessary authenticating intention; and (b) any formalities relating to execution of the document are satisfied – an electronic signature is capable of having legal validity (see the Law Commission's statement of law in the 2019 report on electronic execution of documents) (Law Commission 2019 Report). In determining whether a method of signature demonstrates an authenticating intention, the courts have adopted an objective and pragmatic approach – taking into consideration the circumstances preceding the execution of the document, and any relevant legislative requirements. The law is generally conducive to electronic execution of documents.

There are certain documents which fall under the exception to the general rules outlined above. For instance, agreements relating to wills, lasting powers of attorney or documents that require registration with a public authority that only accepts "wet ink" signatures.

The Law Commission 2019 Report confirmed that English law permits the use of an electronic signature to execute documents, including where there is a statutory requirement for a signature, and that in most instances, electronic signatures can be used as a valid and viable alternative to handwritten ones. The 2019 Report further confirmed that an electronic signature is admissible in legal proceedings (for example to prove or disprove the signatory's intent to authenticate the document). However, there remains a requirement under current law that where a deed must be signed "in the presence of a witness", it requires the physical presence of that witness. This is the case even where both the person executing the deed and the witness are executing or attesting the document are using an electronic signature on an e-signing platform.

The Law Commission has recommended a review of the laws on deeds, addressing the need for some of the formal requirements of witnessing and delivery of the document. The Government indicated its support for the Law Commission's recommendations, and in September 2021 the Ministry of Justice announced the creation of the Industry Working Group on Electronic Execution of Documents to improve standards, reliability and security in relation to electronic signatures. The group published an interim report in 2022, and its final report on 14 March 2023, which addressed: (i) the challenges arising from the use of electronic signatures in cross-border transactions and how to address them; and (ii) how best to use electronic signatures to optimise their benefits when set against the risk of fraud.

Among the challenges noted is the lack of certainty as to whether electronic execution is valid or enforceable in a specific jurisdiction, and a lack of assurance that e-signing solutions and platforms meet different global requirements. The report set down a number of additional recommendations for reform, including recommendations for enhanced certification and self-certification, extensive adoption of e-signature across government departments and organisations, abolition of some of the formalities in relation to deeds (to allow remote witnessing), and the establishment of a permanent body to focus on issues relating to electronic signatures. At the date of writing, the Government has not proposed a bill to enact any of the recommendations.

Enforceability – The second question that needs to be answered is whether electronically signed agreements can be validly enforced. This second question is highly relevant as there is a significant difference between having the ability in law to execute an agreement electronically and being able to enforce that agreement by proving its existence and contents.

Article 25(1) of UK eIDAS Regulation provides that simple, advanced and qualified electronic signatures have legal admissibility. Further, the Article upholds the principle that an electronic signature will not be denied legal effect and admissibility as evidence in legal proceedings solely on the basis that it is in an electronic form or that it does not meet the requirements of a qualified electronic signature. Therefore, under UK law any document which has been electronically executed (including the digital audit trail) will be admissible in legal proceedings before a UK court to determine the authenticity and/or integrity of that document. That said, it will be a question for the court to determine what evidential weight should be given to an electronic signature. Naturally, the more rigorous the requirements for electronic signatures, the more weight will be given by the court when assessing their validity. Thus, documents executed with an advanced electronic signature or a qualified electronic signature will be afforded more evidential weight by the courts.

Specific regime for Scotland – Scotland has a separate legal framework for the execution of documents. Whilst the general position in Scotland matches that of the rest of the UK (i.e. there is usually no prescribed form of signature to execute documents), there are some important caveats. Section 1(2) of The Requirements of Writing (Scotland) Act 1995 (RWSA) sets out certain documents that must be in writing. They include documents relating to land (such as missives, dispositions and leases), gratuitous unilateral obligations and "truster as trustee" trusts. Section 1(2) documents must be signed with an advanced electronic signature to be legally valid, and a qualified electronic signature to be "self-proving" or "probative" (Regulations 2 and 3 of the Electronic Documents (Scotland) Regulations 2014).

Wills and testamentary writings, and certain documents which are submitted to public registries, must be created and signed as traditional (paper) documents.

As a general proposition, any documents that are not covered by section 1(2) may be executed with a standard electronic signature.

In certain industry sectors, it is common for legal advisers to require their clients to use a self-proving signature even if this is not a strict legal requirement. As noted above, in the case of an electronic document, this requires the signatory to sign with a qualified electronic signature.

Qualified electronic signatures are growing in popularity. Since October 2022, it has been possible to submit electronically signed documents to the Register of Deeds (in the Books of Council and Session). These documents must be self-proving and therefore authenticated with a qualified electronic signature. The Keeper of the Registers of Scotland (Jennifer Henderson) has signalled that it will become possible to register electronically signed documents (with a qualified electronic signature) in the Land Register of Scotland and the Register of Sasines, in the near future. In September 2021, the Keeper advised that "the digital registration service will ultimately grow to become the default method of registration in the coming years". She also advised that only qualified electronic signatures will be accepted.

4 Compliance assessment of Adobe Acrobat Sign

4.1 Description of Adobe Acrobat Sign

Cloud solution – Adobe Acrobat Sign is a SaaS-based electronic signature solution that allows users to flexibly manage the document signature process. Adobe Acrobat 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 Acrobat Sign handles user verification and links all the audit information from the signatory to his or her signature in the document. Adobe Acrobat Sign can be used through a web browser, a mobile device, Adobe Acrobat desktop software or through APIs that connect to the user's existing business applications.

To send a document for signature, the user uploads the document to Adobe Acrobat Sign. Adobe Acrobat Sign supports multiple source document formats that can be signed electronically. Users can specify multiple recipients to sign the document, provide a message to the participants and optionally apply additional security controls to the document. Users may decide which type of electronic or digital signature is used. Adobe Acrobat Sign also enables users to manually create form fields and signature position in a document through a simple drag-and-drop web interface. Signatories will be required to fill in the necessary fields and sign in the appropriate places during the signature process.

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

Users of Adobe Acrobat Sign can log in and authenticate themselves through the following types of user identifiers:

- Adobe Acrobat 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 Acrobat 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 Acrobat Sign.

- Google Gmail and Google Apps – Adobe Acrobat 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 stronger access control mechanism can enable SAML SSO to centrally manage their users through their corporate identity system. It enables account administrators to enforce strong access controls and ensure authentication requirements are aligned with the corporate information security policies.

Just as critically, Adobe Acrobat Sign supports several options for the identification of a signatory – who is not necessarily a registered Adobe Acrobat Sign user but may be required to have the identity verified when signing a document.

A baseline level of authentication is achieved by sending an e-mail with a unique URL to the 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 Acrobat Sign user. After having clicked on said URL link, signatories can use a mouse or pre-defined font style to create a facsimile of a handwritten signature on screen, upload an image file (e.g. a scanned signature) or type in their name and click a button (displaying "*Click to sign*") to sign.

In addition, Adobe Acrobat Sign provides enhanced electronic signatures with multi-factor authentication based on Phone Authentication (based on a One Time Password sent via SMS or voice phone call) and Email OTP (based on a OTP sent via the recipient email).

Verified Signatures - Acrobat Sign also offers Verified Signatures, where the identity of the signatory is verified using third-party identity providers: Knowledge Based Authentication, Government ID Verification and Digital Identity Gateway, an integration layer with leading identity verification service including Document ID verification and Electronic Identity schemes like BankID, IDnow, ID.me and OneID.

Digital signatures – Adobe Acrobat Sign supports (i) the use of remote or cloud-based digital signatures by means of digital certificates stored in the cloud by a trust service provider (TSP) and (ii) the use of digital signatures based on locally stored digital certificates in combination with Adobe Acrobat or Acrobat Reader.

During the signing process, the identity of the signatory is cryptographically bound to the document using the certificate and the private key held by that signatory. During the validation process, the reciprocal public key from the certificate is used to both authenticate the signatory's identity and verify that no changes were made to the document since it was signed. Digital signatures are also generated according to the PAdES standard (ETSI EN 319 142) with support for Long Term Validation. In this regard, the audit trail also provides for additional, valuable information such as the signatory's IP address and, where enabled, their geolocation.

The support for digital signatures (advanced and qualified electronic signatures) has recently been expanded for multiple signature support, and it is now possible to define up to 10 digital signature fields for each signatory in the same document, if the sender allows this.

Audit Report – Adobe Acrobat Sign allows real-time visibility into the signature process. Once the document has been sent out for signature, Adobe Acrobat 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 report can be retrieved by users through the Adobe Acrobat Sign dashboard or by a signatory (that is not a user) by clicking on a signature in the signed document. In the default configuration, Adobe Acrobat Sign also attaches the audit report to each executed document.

Document certification – After all signatories have signed the document, Adobe Acrobat Sign certifies the document so that any changes to it will be tamper evident. This document certification is compliant with the *Adobe Approved Trust List (AATL)* program so when recipients download and open the signed filed in Adobe Acrobat or Acrobat Reader, a blue banner is displayed at the top of the document, which certifies that no change has occurred to the document during transit or at any point since the certification was applied.

After all signatories have signed the document, Adobe Acrobat Sign also automatically stores all signed documents in a centralised, secure repository where they will remain easily accessible for a configurable period of time, based on a retention policy. Alternatively, users can configure the service to save completed agreements into their existing document management solutions.

Open standard for cloud-based digital signatures – Adobe adopts and promotes the open standard for cloud-based digital signatures from the Cloud Signature Consortium, of which Adobe is a funding member. The aim of the CSC standard is to define a common architecture, building blocks, and communication protocols for cloud-based digital signature transactions. Thanks to the open-source nature of the CSC API, this standard has been adopted globally by more than 70 members.

Adobe Acrobat Sign is the first SaaS-based electronic signature solution to incorporate the CSC technical specification and consequently to support the use of digital signatures in the cloud. To reach a high level of compliance, signatories are given digital certificates that are stored securely in the cloud by trust service providers. During the signing process, users authenticate with the TSP hosting the certificate and then provide their authorization to use the hosted private key to generate the remote signature. Multiple

authorization methods are supported, from simple PIN code and one-time password (OTP) sent to a registered mobile number via SMS, up to more sophisticated and secure methods including biometric authorization and mobile apps.

Digital Certificates – For the generation of advanced and qualified electronic signatures, Adobe Acrobat Sign works with virtually every digital certificate issued by third party trust service providers, many of which are trusted by Adobe Acrobat Sign through the *Adobe Approved Trust List* (AATL) and the *European Union Trusted Lists* (EUTL). More than 50 providers, including all the leading global and regional TSP, have partnered with Adobe to provide CSC-compliant services for cloud-based digital signatures, but the list is constantly growing.

To get a certificate from a trust service provider, it is necessary for the user to verify his identity with that trust service provider. To obtain a qualified cloud-based certificate remotely, trust service providers often require a webcam and smartphone to run the online identification procedure, or offer a fully-automated enrolment using ID documents supporting Near-Field Communication (NFC) technology or other forms of electronic identification.

Time stamp – Electronic time stamps accurately record the time of the signing event and encrypt that information in the document so that it cannot be tampered with. Adobe Acrobat Sign offers signatories two options to apply such electronic time stamps to their documents.

Adobe is a qualified trust service provider for electronic time stamp services, as a result of which Adobe can deliver qualified electronic time stamps as defined in Article 3 (34) of the EU eIDAS (and UK eIDAS) Regulation(s). The qualified electronic time stamp automatically applied by Adobe guarantees the long-term validity of the signed agreement by locking the signature as well as the document and meets the most stringent requirements of the EU eIDAS and UK eIDAS Regulations in relation to electronic time stamps. In other words, it provides a further security measure in addition to the digital signature, proving its existence at a defined date and time. An electronic time stamp is critical for digital signature compliance because digital certificates can expire or be revoked, while the Adobe-applied qualified electronic time stamp extends the validity of the digital signature to long-term.

Optionally users that may already have a (third-party) time stamp provider in place, Adobe Acrobat Sign also permits users to configure an alternative electronic time stamp service instead of the default service provided by Adobe. This feature can be enabled provided that such third-party time stamp provider is tested and certified by Adobe. Multiple leading time stamp providers have been pre-qualified for being configured in Adobe Acrobat Sign.

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 Acrobat Sign and any related processes. Adobe Acrobat Sign business processes are certified compliant with ISO 270001, SSAE SOC 2 Type 2 and SOC 3, PCI DSS V3.2.1, GDPR, CSA STAR Level 1, FedRAMP Moderate, IRAP and C5.

4.2 How Adobe Acrobat Sign can support compliance with the EU eIDAS and UK eIDAS Regulations

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

(a) Adobe Acrobat Sign meets the European and UK requirements of standard electronic signatures

Requirements – In accordance with the definition of standard "*electronic signatures*" in the EU eIDAS and UK eIDAS Regulations, 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 Acrobat Sign – In regard to the description of Adobe Acrobat Sign as set out above, we conclude with confidence, that Adobe Acrobat Sign meets or even exceeds the requirements of standard electronic signatures:

- *'data in electronic form'* – Electronic signatures created with Adobe Acrobat 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 Acrobat Sign allows uploading multiple source document formats.

- *'used by the signatory to sign'* – Adobe Acrobat 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 Acrobat 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 "*Click here to sign*".;

  – After this has been done, a notice appears that states "By signing, I agree to this document, the Consumer Disclosure and to utilize electronic signatures." together with a button "*click to sign*". Only once the signatory clicks this button and confirms a second time his intent to sign, Adobe Acrobat Sign considers 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 feature without impact on the value of the electronic signature, this 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 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 signifying their consent.

This means, according to Article 25.1 of the EU eIDAS and UK eIDAS Regulations, that an electronic signature produced with Adobe Acrobat 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 4.2(c) below).

Moreover, Adobe Acrobat 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 Acrobat Sign could serve as proof to demonstrate the link between the identity of a signatory and their signature.

- The multi-factor authentication methods – If multi-factor authentication were required of 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 Acrobat Sign is not merely a solution that facilitates the creation of standard electronic signatures in compliance with the EU eIDAS and UK eIDAS Regulations: it is a trustworthy and secure way to do so.

Adobe Acrobat Sign allows one to produce standard electronic signatures in a trustworthy and secure way. Adobe Acrobat 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.

(b) Adobe Acrobat Sign and advanced electronic signatures

Requirements – In accordance with the definition of advanced electronic signatures in the EU eIDAS and UK eIDAS Regulations, 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 Acrobat Sign – If a document is uploaded to Adobe Acrobat Sign for signature, the Adobe Acrobat Sign user can require the signatories to use a digital signature by adding a digital signature form field to the document. A signatory can then choose to download the document to his desktop and sign locally in Adobe Acrobat or Adobe Reader or choose to sign remotely (without download) using a digital certificate issued by and stored by a trust service provider in the cloud.

Desktop deployments – Adobe Acrobat Sign 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 Acrobat Sign, is not legally defined in the EU eIDAS or UK eIDAS Regulations, but must be interpreted as including digital certificate-based advanced electronic signatures and qualified electronic signatures.

When a signatory chooses to sign a document on his desktop, he will be prompted to download the document, which will open in Adobe Acrobat or Adobe Reader (depending on what software 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 Acrobat 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 Acrobat Sign user and the signatories by consulting the signed document itself via Adobe Acrobat Sign or by opening the document directly in Adobe Reader or Adobe Acrobat.

We conclude with confidence that Adobe Acrobat Sign supports the production of digital certificate-based advanced electronic signatures with desktop deployment, as it involves the rather traditional way of creating advanced electronic signatures envisaged by the EU eIDAS and UK eIDAS Regulations.

Cloud-based deployments – Instead of downloading a document and being obliged to make use of a desktop to sign, Adobe Acrobat Sign also offers the option of a cloud-based digital certificate.

When a signatory chooses to sign a document online, a pop-up is shown in Adobe Acrobat Sign and they will be prompted to select their trust service provider and sign in to access their digital certificate(s) in the cloud (for the avoidance of doubt, this sign-in is separate from a possible sign-in to Adobe Acrobat Sign itself). The signatory will then be able to select a certificate, preview the digital signature and add a signing reason. After clicking on "*OK*", the signatory will return to the Adobe Acrobat Sign environment and be requested to "*Click here to sign*" to proceed with the signing process. Hereafter a new pop-up is pushed on the signatory's screen (by the trust service provider), which prompts the signatory to enter their PIN code (protecting the digital certificate as provided by the trust service provider) as well as the one-time password (OTP) associated with the digital certificate, whereby the OTP is generated and delivered to the signatory depending on the technology supported by the chosen trust service provider (this is often done through a registered smartphone app). When the signatory clicks once more on "*OK*", the document is considered signed. Finally, 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 Acrobat Sign user and the signatories by consulting the signed document itself via Adobe Acrobat Sign or by opening the document directly in Adobe Reader or Adobe Acrobat.

In this context, the most challenging condition of the definition of an advanced electronic signature has often been the third one, which requires the electronic signature to be *"created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control"*, as the digital certificate is typically not kept by the signatory but by a third party (i.e. the trust service provider).

Recital 52 of the EU eIDAS and UK eIDAS Regulations may be read as paving the way for the use of cloud-based electronic signature solutions as it states that such solutions 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. This seems to be the case in relation to Adobe Acrobat Sign, as a strong multi-factor authentication method is put in place to ensure the sole control of the signatory over the digital certificate.

Assuming that the specifications set out in the open standard for cloud-based digital signatures are correctly implemented by Adobe Acrobat Sign and the relevant trust service provider and the conditions of Recital 52, i.e. with regard to security, are met, we conclude that Adobe Acrobat Sign supports the production of digital certificate-based advanced electronic signatures in the cloud.

Long-term validity – For the sake of completeness, it must be emphasised that Adobe Acrobat Sign enables signatories to ensure the long-term validity of advanced electronic signatures by adding a qualified electronic time stamp, whether through the use of Adobe's qualified electronic time stamp service or through the use of third party electronic time stamp services.

Digital certificate-based advanced electronic signatures (both with desktop and cloud-based deployments) can be integrated in an end-to-end electronic signature process that is supported by and managed through Adobe Acrobat Sign.

(c) Adobe Acrobat Sign and qualified electronic signatures

Requirements – In accordance with the EU eIDAS and UK eIDAS Regulations, a qualified electronic signature is legally equivalent to a handwritten signature and shall be recognised as such in all other EU member states and the UK. As set out above, the EU eIDAS and UK eIDAS Regulations define 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 EU eIDAS and UK eIDAS Regulations. In regard to the requirements of the EU eIDAS and UK eIDAS Regulations, 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 EU eIDAS and UK eIDAS Regulations.

Adobe Acrobat Sign – Adobe Acrobat Sign does not manage or issue qualified certificates and does not offer qualified electronic signature creation devices, but Adobe Acrobat Sign supports

the production of qualified electronic signatures through its interoperation with qualified trust service providers including those that offer cloud-based qualified certificates.

In line with what is set out above in section 4.2(b) regarding advanced electronic signatures, a signatory can choose to download the document to his desktop and sign with a qualified certificate in Adobe Acrobat or Adobe Reader or choose to sign online (without download) using a qualified certificate issued by and stored by a qualified trust service provider in the cloud.

The considerations and processes set out above in section 4.2(b) regarding advanced electronic signatures apply equally to the use of qualified electronic signatures (both with desktop and cloud-based deployments), provided that references to advanced electronic signatures should be construed as references to qualified electronic signatures. The two main differences are (i) that for generating a qualified electronic signature a qualified certificate needs to be obtained from a qualified trust service provider (which in the case of cloud-based qualified certificates often requires the use of a webcam and smartphone to run the online identification procedure), and (ii) that Recital 51 of the EU eIDAS and UK eIDAS Regulations contains a more explicit approval of the use of remote trust service providers for generating qualified electronic signatures.

For the sake of completeness, it must be mentioned that Adobe Acrobat and Adobe Reader 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 (and is therefore recognised as qualified trust service provider under UK law), 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).

We conclude with confidence that, Adobe Acrobat Sign supports the production of qualified electronic signatures both with desktop and cloud-based deployments.

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

Long-term validity – For the sake of completeness, it must be emphasised that Adobe Acrobat Sign enables signatories to ensure the long-term validity of qualified electronic signatures by adding a qualified electronic time stamp, whether through the use of Adobe's qualified electronic time stamp service or through the use of third party electronic time stamp services.

Qualified electronic signatures (both with desktop and cloud-based deployments) can be integrated in an end-to-end electronic signature process that is supported by and managed through Adobe Acrobat Sign.

5 Conclusion

Adobe Acrobat 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 Acrobat Sign supports a range of options for verifying the identity of the Adobe Acrobat 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 log-in). Moreover, the processes underpinning Adobe Acrobat Sign have been designed in such a way that they clearly capture the intent of the signatories. Finally, to protect the signed document against any subsequent changes, Adobe Acrobat 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.

We conclude with confidence that when the appropriate user settings are selected, Adobe Acrobat Sign is a trustworthy and secure tool that enables the creation of standard electronic signatures that meet or even exceed the requirements of a standard "*electronic signature*" as defined in Article 3 (10) of the EU eIDAS and UK eIDAS Regulations. This means that according to Article 25.2 of the EU eIDAS Regulation and Article 25 of the UK 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 signatures are often considered to be sufficient. When courts need to assess the value of the submitted evidence to them, they will generally give more evidential weight to documents that are electronically signed with more trustworthy and secure technology. In this respect, Adobe Acrobat Sign provides important evidentiary value by providing a multi-factor authentication, registering every single action on Adobe Acrobat Sign and certifying the signed document.

Furthermore, we observe that Adobe Acrobat Sign contains an option supporting the use of digital signature technology, notably advanced electronic signatures as defined in Article 3 (11) of the EU eIDAS and UK eIDAS Regulations and qualified electronic signatures as defined in Article 3 (12) of the EU eIDAS and UK eIDAS Regulations. Hence, if this option, which enables the creation of digital signatures both with desktop and cloud-based deployments, is activated by the user, Adobe Acrobat Sign is an innovative and 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 Acrobat Sign supports the creation of electronic signatures that, in accordance with Article 25 of the EU eIDAS and UK eIDAS Regulations, have the equivalent legal effect of a handwritten signature and is recognised as such in other EU member states and the UK. Moreover, Adobe Acrobat Sign offers reliable means to guarantee the long-term validity of such signatures through Adobe's own qualified electronic time stamp service and through its integration with third party electronic time stamp services.

Adobe Acrobat 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 EU eIDAS and the UK eIDAS Regulations. Adobe Acrobat Sign in particular allows users to configure and build workflows in accordance with the user's specific compliance, industry and risk profile.

Authors

DLA Piper UK LLP (Brussels) has a global intellectual property and technology (IPT) group consisting of 60-plus offices, around 150 partners and 530-plus fee earners in more than 20 countries, constituting the world's largest IPT team. With over 120 lawyers based in our office in Brussels and our working hub in Antwerp, DLA Piper in Belgium combines DLA Piper's global reach with local know-how. More specifically, the IPT team is part of a global, fully integrated group of IPT teams that operate in the markets of greatest importance to the firm's multinational clients. The Belgian team continuously develops innovative processes and methodologies to improve the delivery of legal services to its clients, as well as the internal organisation of its clients. The whole IPT team is fully dedicated to advising on IT, media and telecommunications matters, acting for both customers (larger users of IT) and large IT vendors, which gives it invaluable insight at both sides of the negotiation table, translating into better, more commercial and more pragmatic advice for its clients.