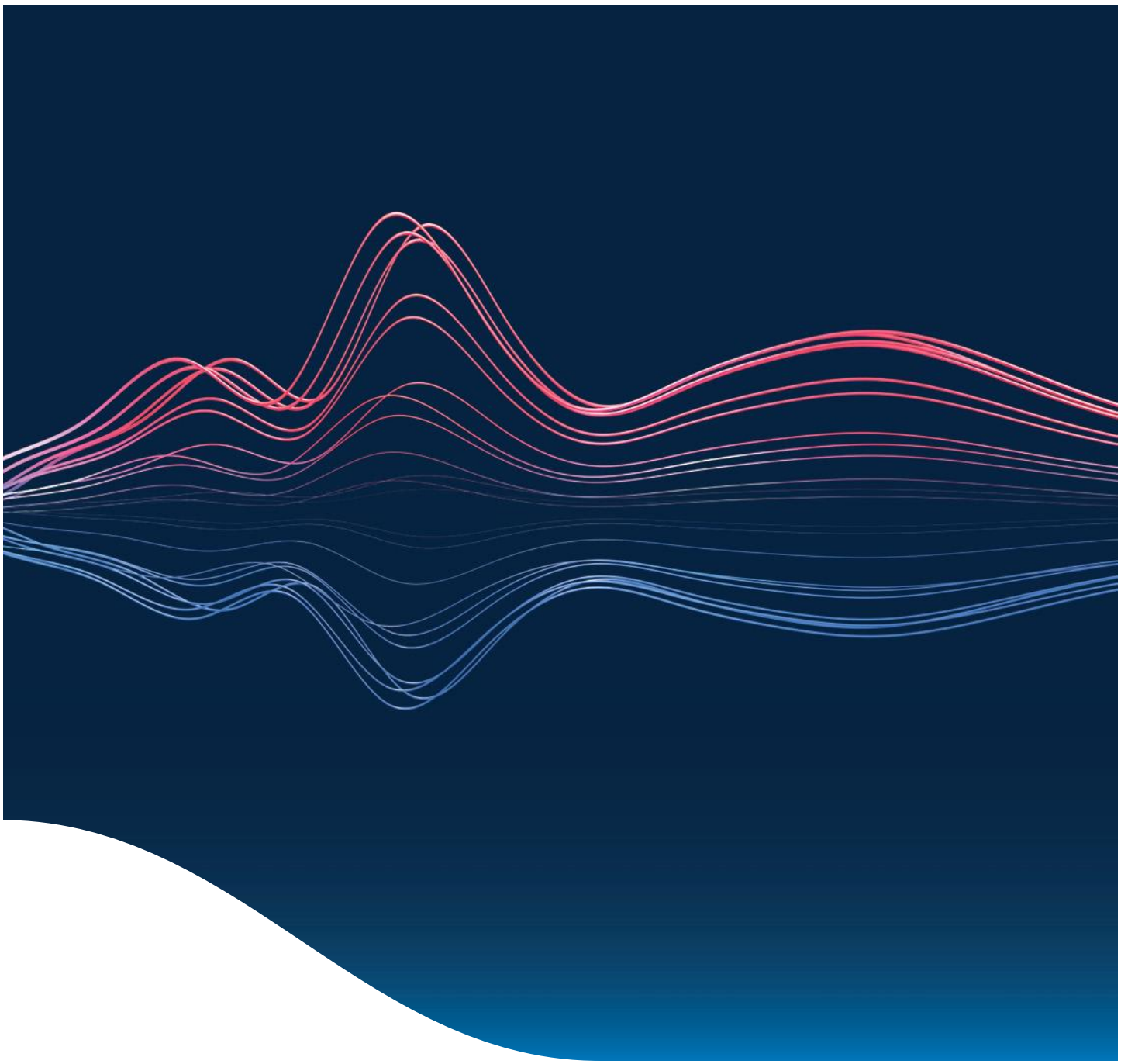

Connective eSignatures

Legal Compliance Assessment

DLA PIPER

Contents

1. Introduction

This white paper contains an analysis of the legal effectiveness of the Connective "*eSignatures*" solution (hereinafter **Connective eSignatures**). In the first part, we describe the key features of the Connective eSignatures solution. The second part of this white paper addresses the compliance of the Connective eSignatures with electronic signatures rules.

European Union - Based on our analysis, if it is properly configured, Connective eSignatures allows the creation of electronic signatures within the meaning of Article 3(10) of the eIDAS Regulation and even, depending on the signature method chosen by the customer or user, certain advanced and qualified electronic signatures (within the meaning of Articles 3(11) and 3(12) of the eIDAS Regulation). Connective has also included in Connective eSignatures means guaranteeing the long-term validity of these electronic signatures, namely an integration with third-party electronic time-stamping officially recognised certificate authorities (CAs).In this context, and with proper configuration, Connective eSignatures as an electronic signature solution allows the management of a signing process that complies with the requirements for all kinds of electronic signatures foreseen under the eIDAS Regulation.

Switzerland - Based on our analysis, if it is properly configured, Connective eSignatures allows the creation of electronic signatures within the meaning of Article 2(a) of the FAES. However, none of the analysed signing methods meets the requirements of a regulated electronic signature and qualified electronic signature (as defined in Articles 2(c) and 2(e) FAES) because Connective eSignatures are not certified by an accredited conformity assessment body in Switzerland, nor do the signing methods use (regulated or qualified) certificates issued by a body which is certified in Switzerland.

United States - With its breadth of signing methods supported, Connective eSignatures allows the initiator of the signing process to choose the settings that are most appropriate to the electronic document in question and the intended legal consequences. With this properly done, we conclude with a high level of confidence that Connective eSignatures is a tool that, in conjunction with appropriate and legally compliant processes, allows the production of electronic signatures and records with respect to certain transactions, each as defined in the U.S. eCommerce Laws.

Hong Kong - Connective eSignatures meets the requirements for an electronic signature under the ETO. As a result, an electronic signature produced with Connective eSignatures on a document can, in principle, not be denied legal effect, save for certain exempted documents which cannot be signed electronically such as land agreements.

Singapore - Connective eSignatures is a tool that, in conjunction with appropriate and legally compliant processes, allows the production of electronic signatures and secure electronic signatures as defined in the ETA. Connective eSignatures does not meet the requirements for digital signatures under the ETA.

Note: this analysis is purely intended as a legal assessment under the rules of the eIDAS Regulation, Swiss Federal Act on Electronic Signatures, the U.S. eCommerce Laws, the Electronic Transactions Ordinance and the Electronic Transactions Act is not a technical assessment in any way.

2. Description of Connective eSignatures

Cloud solution - Connective eSignatures is a cloud-based **Software-as-a-Service electronic signature solution** that allows users to manage the signing process for a document, from upload to signing and sealing. Connective eSignatures can be used on various devices, including mobile devices and computers, through an app or a web browser, and can also be integrated within other applications through the use of Connective's own APIs. Connective eSignatures handles user verification for most of the signature methods, and incorporates certain data into the signature in the document.

Configuration options - To start the signing process, the user uploads a document onto Connective eSignatures (e.g. a PDF file; several formats are supported), whether from his or her device or from a supported cloud hosting solution (e.g. Dropbox, Google Drive or OneDrive). The user can then specify a category of document, language and legal notice that can be defined on an individual signatory level (e.g. when a signatory needs to fill in "*Read and approved*"). Afterwards, the user identifies the location of the signature fields and signatories (giving certain information on the signatory's identity, with at a minimum name and e-mail address), as well as - per signatory and signature field - the available signature methods and, if needed, a legal notice on individual signatory level. If a specific signing sequence is required (e.g. a is required to sign before B), this can also be specified. Finally, Connective eSignatures includes features such as an expiry date (on which the document becomes inaccessible), signature tracking (to verify at any time which signatures are missing) and automatic reminders.

Start of the signing process - After configuring the electronic documents for signature, an email is sent to the signatory inviting him or her to click on a link in the e-mail to electronically sign the document. When a signatory clicks the link in the email signing invitation, the electronic documents for signature are displayed in the WYSIWYS (What You See Is What You Sign) interface of Connective eSignatures. The WYSIWYS interface includes a button on the left side which states "*Reject*". The signatory can click "*Reject*" and insert his/her reason for rejection at any time before signing is completed to decline to sign the electronic documents. Additionally, the WYSIWYG interface includes a button on the left side which states "*Download*". Clicking this button allows the signatory to download all documents in unsigned form for review prior to execution.

The WYSIWYS also displays in the documents the signature locations for all signatories, indicating the available signing method or methods chosen by the initiator for execution of the electronic document. The signatory must first scroll through the entirety of all the electronic documents posted in Connective eSignatures for review and execution before the bottom of the WYSIWYS activates a click box which states "*I declare that I have read all documents and I agree with the "**Privacy Policy**" and "**Cookie Policy**"*". Connective eSignatures requires the signatory to click the hyperlink for the "*Terms of use*" to view this document before the second click box becomes active.

Authentication - Authentication is a two- and sometimes three-step process.

1. When using Connective eSignatures, the initiator of the signing process (the user uploading the document) has to provide information on each signatory to allow Connective to send that user a notification that a document is available for signature.
2. Afterwards, Connective eSignatures verifies the signatory's identity from the perspective of access to the document. By default, this 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. After having clicked on said URL link, signatories can create a facsimile of a handwritten signature on screen (e.g. using a mouse, stylus or their finger) and click a button (displaying "*sign*") to sign.

3. The third stage of authentication occurs when using anything other than the most basic signing method (i.e. anything other than "*manual*" signing) which include the following:

Manual Signing	No additional verification at signing time.
E-mail OTP (one-time password)	Additional verification of the signatory's email address via a one-time password sent to the email address which has been provided by the Connective eSignatures initiator.
SMS OTP	Additional verification of the signatory's mobile phone number via an OTP sent to the mobile phone number which has been provided by the Connective eSignatures initiator. If no mobile number has been registered in Connective eSignatures, the SMS OTP signing option will not be available.
Biometric	No additional verification at signing time, however the biometric data of the signatory is included in the signature image, which can in dispute afterwards be made available to a forensic expert, who can use this data and a specific tooling to verify and compare this with other signatures of the same person.

Digital signatures - Connective's certificate is cryptographically bound during the signing process to the document using the private key held by Connective, in order to preserve the integrity of the document.

Audit trail - Connective eSignatures allows **real-time visibility** into the signature process, by giving the initiator access to a dashboard showing the signature status. This functional logging features information on when a document was uploaded, when it was signed, which signing method was used, the status of the signature process, the list of all signers and the list of all receives. After dispatch of the document for signature, Connective eSignatures handles automatic reminders and signature tracking to facilitate the signing process.

Each (key) step in the signing process is also captured in an audit trail that is secured and that provides evidence in a clear format, easily produced, of each signatory's signature. Such information includes notably the functional logging information mentioned above, as well as more detailed information on the process (e.g. if a reminder was sent, time of the reminder, content and recipients; if an SMS was sent, time, content and recipient) and on the signatures (signature certificate, chain and certification list; timestamp certificate, chain and certificate revocation list; extra proofs set by the Connective eSignatures client; …). Such data is stored in XML files signed by Connective. This audit trail is by default only available to the administrator.

Document certification - After the carrying out of one of the above-mentioned actions and authentications, the document will be sealed with the Connective EUTL (European Trust List) certificate or Connective AATL (Adobe Approved Trust List) certificate and information related to the transaction is embedded into the seal.

Connective eSignatures automatically certifies a final PDF of the signed document before distributing it to all participants. When recipients download and open the signed filed in a PDF viewer with certificate reading capabilities, a 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, Connective eSignatures also automatically stores all signed documents in a centralised, secure repository where they are easily accessible, and it works with an external partner for the transition towards electronic archiving. In addition, the Connective eSignatures API allows the integration of Connective eSignatures within other platforms such as document management solutions, ERPs, core banking systems, etc.

Time stamp - Electronic time stamps record the precise time of signing and encrypt that information in the document to prevent tampering. Connective eSignatures works with a certificate authority (appearing on the relevant Member State trusted lists) to provide time-stamping. For regional reasons, Connective eSignatures can be configured to work with a specific, local time-stamping authority where required by the partner or customer. Connective always advises to use a qualified time-stamping service to be able to guarantee the correctness of the time stamps and therefore their legal value.

Cloud security - Within Connective eSignatures and throughout its own organisation, Connective has deployed a range of technical and organisational measures to protect the security and confidentiality of all data and documents entrusted to Connective. This includes for instance client-side encryption (so that the storage component never sees unencrypted data), as well as adherence to various security standards (ISO 27002 and ISO 27005, ETSI EN 319401 and ETSI EN 319102 as well as where relevant the XAdES, PAdES and CAdES recommendations (ETSI EN 319 122-1, 122-2, 132-1, 132-2, 142-1, 142-2).

3. European Union

In this chapter, we first give an overview of the relevant electronic signature rules in the European Union. Then, we reflect on the validity and enforceability of electronic agreements in the European Union. Finally, we analyse the legal effectiveness of Connective eSignatures in light of the applicable legal framework.

3.1 Electronic signature rules

eSign Directive - The previous legal framework on electronic signatures in the EU was Directive 1999/93/EC (the **eSign Directive**). One of the biggest shortcomings of the eSign Directive was the lack of interoperability between electronics signature solutions in different EU Member States. While the Directive specified the legal effects of electronic signatures, it did not include any provisions for ensuring acceptance in one EU Member State of an electronic signature already recognised in another. It was therefore highly uncertain whether electronic signatures would be accepted in cross-border electronic transactions, even within the EU.

On 23 July 2014, the eSign Directive was repealed and replaced by Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the **eIDAS Regulation**). In that way, the European legislator hoped to boost the use of electronic signatures and other trust services (such as electronic time-stamping services), and to contribute to the creation of a digital single market.

eIDAS Regulation - The fact this is a regulation instead of a directive has important consequences as a regulation does not need to be transposed in the EU Member States' national laws but is directly applicable in all EU Member States. Consequently, businesses are no longer confronted with varying national electronic signatures laws.

The eIDAS Regulation nevertheless has some of the same limitations as the eSign Directive: while it aims to ensure the legal effectiveness of electronic signatures and their admissibility as evidence in legal proceedings, the conclusion and validity of (electronic) agreements remains a matter of national law (see section 3.2 below).

In the eIDAS Regulation, next to the broad concept of "*electronic signature*", there are two additional variants, namely "*advanced electronic signatures*" and "*qualified electronic signatures*".

3.1.1 SIMPLE ELECTRONIC SIGNATURES

Broad definition - A simple "*electronic signature*" or **SES** is defined broadly in the eIDAS Regulation. According to Article 3(10) of the eIDAS Regulation a SES is 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. No reference is made to a specific technology.

Recital 26 to the eIDAS Regulation clarifies that because of the pace of technological change, the eIDAS Regulation should adopt an approach which is open to innovation. In addition, Recital 27 explicitly states that the 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 eIDAS Regulation are met.

We can infer three criteria from the definition of an "*electronic signature*" in the eIDAS Regulation, namely: (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. The eIDAS Regulation does not further define or explain these criteria, and thus leaves room for interpretation and technological innovation. In practice, "*electronic signature*" can cover a broad range of electronic tools that capture the intent of the signatory to approve the content of a document. This may include PIN codes, one-time passwords, e-mail signatures, electronic identity cards, scanned signatures, symmetric or public key cryptography signatures and biometric signatures.

Legal effect - Article 25(1) of the eIDAS Regulation states that an electronic signature **cannot be denied legal effect and admissibility as evidence** in legal proceedings solely on the grounds that it has an electronic form or that it does not meet the requirements for qualified electronic signatures. As a consequence of this provision, EU Member States cannot adopt or maintain legislation that rejects the legal effect or admissibility as evidence of electronic signing tools solely because of their electronic format or non-qualified nature.

The fact that a simple "*electronic signature*" may not be denied legal effect and admissibility as evidence based on certain technical characteristics does not necessarily mean that it will receive the same legal treatment as a handwritten signature. National rules regarding the free consideration of evidence by courts also remain unaffected.

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.

3.1.2 ADVANCED ELECTRONIC SIGNATURES

Four technology-neutral criteria - An "*advanced electronic signature*" or **AES** is described in Article 3(11) of the eIDAS Regulation. According to this provision, an AES is a simple "*electronic signature*" that meets the requirements of Article 26 of the eIDAS Regulation, i.e. (i) it is uniquely linked to the signatory; (ii) it is capable of identifying the signatory; (iii) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (iv) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable. The definition of an AES is therefore technology-neutral. By way of further confirmation, Recital 26 to the eIDAS Regulation affirms that the eIDAS Regulation is or should be open to innovation, and Recital 27 adds that the legal effects it grants should be achievable by any technical means.

Public-key cryptography - Nowadays the term "*advanced electronic signature*" is used mainly to refer to electronic signatures that are based on digital signature technology that make use of **public-key cryptography**. In this context, such signature will be seen as a digital file containing a hash of the document obtained by encryption with the private key of the signatory. The corresponding public keys enable the verification of this signature. The digital certificate, particularly an electronic attestation, which links the data for validating the signature to a natural person and verifies at least the name or the pseudonym of that person, confirms that the signatory is the owner of the public key in question.

Remote signatures - As a result of the technology-neutral definition of an AES, other technologies that make it possible to produce an AES are not excluded, provided that the four aforementioned requirements are met. For instance, Recital 52 specifically mentions the creation of **remote electronic signatures** through an electronic signature creation environment managed by a trust provider on behalf of the signatory. According to this Recital, remote electronic signatures should receive the same legal recognition as electronic signatures created in an entirely user-managed environment, on the condition 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 Recital 52, a signatory could choose to store his private key in the cloud, provided that the four abovementioned conditions are fulfilled. It may even be possible for the signatory to use a cloud-based electronic signature solution that does not require any signatory keys at all.

Increased level of trust - The eIDAS Regulation does not grant any legal effect to an AES different from the legal effect granted to a SES. The notion nevertheless serves as a building block in the definition of a qualified electronic signature (see section 3.1.3 below).

An AES, such as a PIN code or a scanned signature attached to a document, is also generally considered to be of a higher technical security level. Hence, AES are normally recognised as being more trustworthy and possessing a higher evidential value in judicial proceedings. However, the technical method used is only one of the elements that will be taken into account by court. Consequently, the trustworthiness of a specific digital certificate-based electronic signature can be questioned in one particular case, while the court may decide in another case that a PIN code provides sufficient evidence.

Although the legal effects of advanced electronic signatures are not different from those for simple electronic signatures, advanced electronic signatures are generally considered to be more trustworthy and to possess a higher evidential value in legal proceedings. Moreover, the eIDAS Regulation seems to pave 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.

3.1.3 QUALIFIED ELECTRONIC SIGNATURES

Extensive set of criteria - The definition of a "*qualified electronic signature*" or **QES** is contained in Article 3(12) of the eIDAS Regulation, which states that a QES is an AES that is created by a QES creation device, and which is based on a qualified certificate for electronic signatures.

Article 3(15) of the eIDAS Regulation specifies that a qualified certificate for electronic signature means a certificate for electronic signatures that is issued by a qualified trust service provider and meets the requirements laid down in Annex I to the eIDAS Regulation. 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. For QES, this means in practice the commercial or governmental certificate authority that certifies the ownership of a named person's public key by issuing a digital certificate.

In addition, a QES must be created by a QES creation device. Annex II to the eIDAS Regulation sets out requirements to be met to safeguard the trustworthiness of data on such a device, and the software or hardware (e.g. a smart card or a USB token) used to create the signature must comply with these requirements.

Remote signatures - With respect to QES, Recital 51 to the eIDAS Regulation clearly states that QES creation devices (e.g. a cloud-based hardware security module) can be entrusted to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his or her electronic signature creation data (e.g. his/her digital certificate) and the QES requirements are met by the use of the device (e.g. through a mobile app).

Equal to handwritten signature - Article 25(2) of the eIDAS Regulation describes the legal effect attributed to a QES. Under that provision, a QES is **automatically deemed equal to a handwritten signature** and has the equivalent legal effect. Moreover, based on Article 25(3), a QES based on a qualified certificate issued in one EU Member State must be recognised as a QES in all other 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. Moreover, the eIDAS Regulation contemplates the possibility of remote, cloud-based qualified electronic signatures, whereby a third-party trust service provider manages the electronic signature environment on behalf of the signatory.

3.2 Validity and enforceability of electronic agreements

Next to the question of the legal effectiveness of electronic signatures, questions arise in relation to (i) the validity of an electronically signed agreement and (ii) the evidentiary value and enforceability of an electronically signed agreement.

Validity - In order to answer the first question, we should examine the formal requirements that need be fulfilled in order to validly conclude an agreement. "***Consensualism***" is a fundamental principle in European contract law according to which (a) the freely given and mutual consent of the contracting parties suffices to conclude a valid agreement and (b) no formal requirements, such as a written document, registration or signatures, are required. In this context, a signature is merely an embodiment of such consent, rather than a requirement for validity of the agreement.

Agreements can be entered into verbally, in writing, electronically or even implicitly. However, various EU Member States have introduced exceptions to this fundamental principle. This has for instance been the case in certain countries with respect to public procurement agreements, real estate agreements, consumer agreements, settlement agreements and agreements of suretyship. While exceptions certainly 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 - Next to validity, one must check whether agreements can be validly enforced, as there is a significant difference between concluding a valid agreement and being able to enforce that agreement by proving its existence and contents.

Each EU Member State has its own rules concerning the evidentiary value and enforceability of agreements. In civil law countries such as Belgium, France and Italy, the nature of the relationship between the parties has an impact on the degree of freedom in proving the agreement. In B2B disputes, any form of evidence (e.g. any type of writing, testimony, e-mail or factual element) will be admissible. It of course remains up to the court to assess the evidentiary value of the submitted evidence. In B2C or in disputes between private persons, the forms of evidence that are allowed are regulated. For instance, if a dispute is valued above a certain monetary amount, only a signed agreement (this is a written document signed by the parties undertaking obligations) will be accepted as evidence.

Most jurisdictions however allow a contractual deviation from the rules of evidence. This implies that parties can contractually agree which means of evidence will suffice, and/or which evidentiary value is attributed to certain documents. To illustrate, online banking services often foresee in their terms and conditions that users agree that where they confirm a transaction with a card reader, this electronic signature will be considered to meet the functional requirements of a handwritten signature.

Finally, even when evidence is regulated (e.g. in B2C transactions), other evidence (e.g. e-mails describing the content of an agreement) is typically given at least basic evidentiary value, whether by law or in practice.

While there are differences among EU Member States, it is reasonable to state that (i) the vast majority of agreements do not require any formalities to be valid and (ii) for most contractual disputes any evidence (e.g. any type of electronic signature) is admissible with a view to demonstrating the enforceability of an agreement.

3.3 Connective eSignatures compliance assessment

3.3.1 CONNECTIVE ESIGNATURES MEETS THE EUROPEAN REQUIREMENTS OF SIMPLE ELECTRONIC SIGNATURES

Requirements - In accordance with the definition of simple "*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.

Connective eSignatures - Based on the above description of Connective eSignatures, we conclude with confidence that Connective eSignatures **meets and often exceeds** the requirements for a simple electronic signature:

- *'data in electronic form'* - Electronic signatures created with Connective eSignatures 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 Connective eSignatures allows uploading multiple source document formats.
- *'used by the signatory to sign'* - Connective eSignatures 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 your document or package with name* [Name of the document or package]", with the following wording before the hyperlink to Connective eSignatures: "*Please click on the link below to sign your document or package* [Name of the document or package]";
  - when the signatory reviews the document, he is requested to sign the document (the exact method - creating a "*handwritten*" signature on screen, e-mail confirmation, etc, depends on the signing method). The placeholder for that signature is a form field in the document entitled "*Your signature here* [name]";
  - clicking that field brings up a popup screen stating that "*To start the signing process: read and scroll through all documents, declare that you have read all documents and click "Start signing" at the bottom of the page.*";
  - in order to sign a document, the signatory must therefore first scroll through the entire document, tick a box stating "*I declare that I have read all documents and shall comply with the following policies*" and then click on a button stating "*Start signing*";
  - the signatory is then guided through the signature process that applies to the relevant signing method, typically in two stages under the signatory's control (e.g. inputting the signatory's e-mail address for e-mail OTP signing, then submitting the OTP sent by e-mail) followed by a final stage without signatory involvement, namely the integration of the signature within the document;
  - Connective eSignatures only considers the document to have been signed by that signatory once these three stages have been completed. Connective eSignatures then informs the initiator of the signing process of the fact that the signatory has signed the document.

The third criterion is therefore met, not as a result of the signature's appearance within the final document (which can be seen as a merely visual, esthetical feature without impact on the value of the electronic signature), but because of the multi-faceted approach to capturing the intent of the signatory to sign. This process is moreover important in the context of the formation of a contract between parties, as mutual consent between parties is the element that as a rule creates a contractual relationship between them. In the case of a contractual document being signed, therefore, a **clear signature process** (with notably the requirement to read the entire document before signing becomes possible) helps demonstrate the **willingness of the signatory to be bound by the legal obligations set out in that document**.

As a result, in accordance with Article 25(1) of the eIDAS Regulation, an electronic signature produced with Connective eSignatures can, in principle, not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds of its technical features. This does not mean, however, that such an electronic signature automatically acquires the same legal validity as a handwritten signature. This will be reserved for the situations where a qualified certificate is used (see section 3.3.2 below).

In addition, the audit trail and multi-factor authentication methods used within Connective eSignatures further **strengthen the enforceability** of even "*basic*" signing methods, compared to other commonly accepted electronic signatures:

- **Audit trail:** in case of any dispute regarding the validity of the electronic signature, the audit trail generated by Connective eSignatures would be useful evidence to show the link between a signatory and a signature.
- **Multi-factor authentication methods:** where imposed on the signatory, multi-factor authentication increases the ability to properly authenticate the signatory and produce electronic signatures with an increased evidentiary value.

Finally, Connective eSignatures implements specific **security and technical measures** to ensure that the data to be signed is not altered prior to signature, irrespective of the signing method chosen. Each page of the document to be signed is converted to an image to ensure that it cannot be altered, even before displaying it to the signatory. The data communication between the signatory and the application is done using an encrypted tunnel (HTTPS). The communication protocol of the application uses a security token to ensure no replay is possible.

Connective eSignatures is therefore not merely a solution that allows one to produce simple electronic signatures in compliance with the eIDAS Regulation; in reality, it intends to make available additional layers to create greater trust and security.

Connective eSignatures allows one to produce simple electronic signatures. In addition, it strives to increase trust and security by (i) allowing advanced identification of the signatories, (ii) capturing the intent to sign in an unambiguous way and (iii) supporting the enforcement of the resulting electronic signature through its audit trail.

3.3.2 NATURE OF SIGNING METHODS SUPPORTED BY CONNECTIVE ESIGNATURES - EU-WIDE

Different signing methods, different classification - As described previously, the eIDAS Regulation makes a distinction between **qualified** electronic signatures (**QES**), **advanced** electronic signatures (**AES**) and all other, "*simple*" electronic signatures (**SES**).

In order to assess whether Connective eSignatures allows the use of methods meeting the requirements of an advanced or even qualified electronic signature, it will be worthwhile examining each method in turn.

By way of a reminder:

- as indicated in section 3.3.1 above, the whole Connective eSignatures platform meets (and even exceeds) the requirements for **SES** under the eIDAS Regulation. This assessment applies to all signature methods supported by Connective eSignatures;
- an **AES** must be:
  - uniquely linked to the signatory;

- capable of identifying the signatory (this requirement is easily met by all signing methods explained hereunder);
- created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control (*this is typically the most challenging of these requirements, as "sole control" involves being able to establish that, with a high level of confidence, only the signatory could produce the digital signature in question*);
- be linked to the data signed therewith in such a way that any subsequent change in the data is detectable (*this requirement is met through the audit trail and AATL certificates mentioned earlier*);

- a **QES** must be an AES that, in addition, is:
  - based on a qualified certificate (*issued by a qualified trust service provider and meeting the requirements of Annex I to 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*);
  - created by a qualified electronic signature creation device (*configured hardware or software [e.g. a smart card, a USB token, a cloud-based hardware security module, …] used to create an electronic signature and meeting the requirements of Annex II to the eIDAS Regulation*).

Preliminary note on identification of the signatory - Before examining each signature method, it is important to note that of all the signature methods, half rely solely on the information given by the initiator of the signing process in order to identify the signatory, while the other half benefit from third-party confirmation of identity. This will be discussed for each signing method below.

Manual signing - The "*manual signing*" method meets the SES requirements. However, the first and third AES conditions ("*uniquely linked*" and "*sole control*") present a challenge, given that any other person could recreate a scribble that is indistinguishable from the signatory's (in particular as a result of the imprecision inherent in drawing a signature with a mouse, if a mouse is used). Unlike with handwritten signatures, the imprecision of a digitally drawn signature (in this particular signing method) creates a lack of detail that limits the **unique link** of the signature with the signatory as well as the **sole control** over the signature creation data (in this particular case, the method for reaching the end result of the signature). Moreover, manual signing (like certain other signing methods) relies solely on the information provided by the initiator in order to verify an individual's identity; as a result, there is no means integrated within the signing method itself or the signature process more broadly that can help mitigate these limitations. Recognising these limitations, Connective itself recommends to only use manual signing in the context of face-to-face signing sessions. Therefore, "*manual signing*" fails the AES test (and therefore also the QES test).

E-mail OTP - The e-mail OTP (one-time password) method also meets the SES requirements. As with manual signing, e-mail OTP relies on information provided by the initiator to verify the signatory's identity. However, the use of an OTP (six digits long, reset any time the signatory requests a new one) sent to the e-mail address indicated by the initiator as the signatory's address can be viewed as reaching a higher level of security than the manual signature method. However, because the OTP itself is generated by Connective eSignatures, the "***sole control***" condition must be deemed not to be met. Therefore, e-mail OTP must in our view be considered to be a strengthened SES, but not yet an AES or QES *(though see in this respect the section on "**Transforming a SES into an AES**" below)*.

SMS OTP - The SMS OTP (one-time password) method is similar to the e-mail OTP method. The key difference between SMS OTP and e-mail OTP is that SMS OTP involves an additional authentication factor (a mobile phone, on top of the e-mail address that is necessary for receipt of the link to access the document). However, while this additional authentication factor further increases the level of uniqueness, the "***sole control***" criterion remains problematic. As a result, the SMS OTP method is among the most advanced SES methods available through Connective eSignatures, but it does not in our view meet the requirements for an AES or QES *(see also section on "**Transforming a SES into an AES**" below)*.

Biometric - Biometric signatures are placed with tablets (currently Wacom tablets), which provide a specific layer, meaning that all signatures placed on any of the supported tablets will be recorded in the same way. When using such a biometric signature, the biometric data and other relevant transactional information is stored in the signature of the signatory. In case of dispute this could be used in combination with a specific application of the tablet manufacturer and a forensic expert to verify and analyse whether a person has signed a document or not. As a result of the captured information in relation to biometrics, the biometric signatures used within Connective eSignatures can be deemed to be **uniquely linked** to the signatory. In addition, as the manner of signing is specific to each individual, the data for signing (the image combined with the biometrics themselves) can be considered to be under the signatory's **sole control**. This (combined with the two other criteria for an AES, which are more easily established in the case of all Connective eSignatures signing methods) leads us to conclude that the biometric signing method in Connective eSignatures can be viewed as an **AES**. However, in the absence of any certification, it will not be able to qualify as a QES.

Transforming a SES into an AES - Some of the signing methods examined above are therefore by default classified as **SES** and not AES, in particular where they are not normally able to meet the AES requirement of "*sole control*". However, it may be possible for an onboarding procedure that increases the confidence of sole control over the signature creation data to **transform a SES into an AES**. It is therefore crucial to examine in practice whether the particular implementation at the level of onboarding of e.g. e-mail or SMS OTP could be sufficient to create sole control "*with a high level of confidence*".

In other words, **without additional onboarding**:

Signing method	SES	AES	QES
Manual signing	✓	✗	✗
E-mail OTP	✓	✗*	✗
SMS OTP	✓	✗*	✗
Biometric	✓	✓	✗

* See section on "***Transforming a SES into an AES***" above

Long-term validity - For the sake of completeness, it is worth reiterating that time-stamping services (provided by an external certificate authority) allow signatories to ensure the long-term validity of electronic signatures.

Choice between signing methods - Given that the different signing methods are classified differently under the eIDAS Regulation, it is recommended for users of Connective eSignatures that they verify which settings are most appropriate in the light of the nature of the document and desired legal consequences, in particular

given that certain kinds of documents can only be validly signed through the use of a qualified electronic signature. Connective eSignatures supports all methods, but the choice of appropriate signing method is left to the initiator of the signing process.

Connective eSignatures allows the use, depending on the choices of the initiator of the signing process (based on the nature of the document and desired legal consequences), of simple and advanced electronic signatures, in a manner that enables long term validity of such signatures.

3.3.3 NATURE OF SIGNING METHODS SUPPORTED BY CONNECTIVE ESIGNATURES - BELGIUM

The Belgian eID, lawyerID and itsme® can be used as authentication methods in Connective eSignatures. These authentication methods all go beyond the most basic signing method (i.e. anything other than "*manual*" signing) as described below:

Belgian eID (and "*manual + eID*" method)	Pin code to unlock the private key on the smartcard. Extra signatory validation is possible, through checking the NRN (national registry number - the use of which is strictly regulated in Belgium) or a combination of name, first name and birthdate at signing time.
LawyerID	Pin code to unlock the private key on the smartcard. Extra signatory validation by checking the Lawyer UID (unique lawyer ID) at signing time can be configured
itsme®	Unique validation code sent to the user's itsme app, and authorisation within itsme needed to allow the transaction to go further.

For the Belgian eID and LawyerID signing methods, the signatory's certificate is cryptographically bound during the signing process 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.

Belgian eID (and "*manual + eID*" method) - Connective eSignatures allows the initiator to select two signing methods that involve the Belgian eID (digital identity card). The first involves only eID signing, while the second combines eID signing with the "*manual signing*" method described previously (as an additional visual layer without any impact from a legal perspective). The Belgian eID was conceived as a **QES** from the outset. It has FEDICT, the IT department of the Belgian government, as its root **certificate authority**, and requires the use of an eID card reader, which is a **qualified electronic signature creation device**. In relation to the AES criteria (which also form part of the QES requirements), with the eID, there is notably a **unique link** with the signatory (through the uniqueness of the certificate for each individual) and sole control by the signatory (through the need for physical possession of the eID card and knowledge of the PIN code of that eID card). To sign using eID, the signatory has to connect a card reader to his or her device (as well as download the relevant eID and Connective eID browser packages) and authenticate using his or her PIN

code through the eID browser package or card reader directly (depending on the card reader). After authentication, the eID certificate will be read and integrated in the signature.

LawyerID - The LawyerID signing method is a **QES** that is created through the use of a lawyer card issued by the company Zetes SA/NV (appointed by the Belgian bar associations). The LawyerID signing method is an additional functionality of such lawyer cards that, depending on the bar association, has to be activated separately (for a fee). It features Zetes as its root **certificate authority** for the LawyerID, and requires the use of specific card readers supported by Zetes (all of which are **qualified electronic signature creation devices**). In relation to the AES criteria (which also form part of the QES requirements), with the LawyerID, there is notably a **unique link** with the signatory (through the uniqueness of the certificate for each lawyer) and sole control by the signatory (through the need for physical possession of the LawyerID card and knowledge of the PIN code of that LawyerID signature function, which moreover is by default different from the PIN code for the LawyerID card itself). To sign using LawyerID, the signatory has to connect a card reader to his or her device (as well as download the relevant Connective browser package) and authenticate using his or her PIN code through the browser package or card reader directly (depending on the card reader). After authentication, the LawyerID certificate will be read and integrated in the signature.

itsme® - Originally intended for authentication only (and initially mainly for banks), itsme is a mobile application developed by the company Belgian Mobile ID SA/NV. In September 2018, electronic signing functionality integrated within itsme gained **QES** status through the recognition of Belgian Mobile ID as trust service provider in Belgium for electronic signatures. This signing functionality features Belgian Mobile ID SA/NV as its root **certificate authority**, and it requires the use of an application on a smartphone uniquely linked to the signatory (the combination of which will be considered a **qualified electronic signature creation device**). In relation to the AES criteria (which also form part of the QES requirements), with itsme, there is notably a **unique link** with the signatory (through the fact that the identity in itsme is controlled by the bank that first validates the account or the Belgian Government if the Belgian eID option is chosen to onboard to itsme, and that each individual's profile on itsme is unique) and sole control by the signatory (through the need for physical possession of the mobile device on which the application is installed and some authentication method [fingerprint or PIN code] for authentication). To sign using itsme, the signatory has to open the itsme mobile application and confirm, after authentication, the signature request from within the itsme mobile application. After such confirmation, the itsme signature certificate will be read and integrated in the signature.

Signing method	SES	AES	QES
Belgian eID	✓	✓	✓
Manual + Belgian eID	✓	✓	✓
LawyerID	✓	✓	✓
itsme	✓	✓	✓

3.3.4 NATURE OF SIGNING METHODS SUPPORTED BY CONNECTIVE ESIGNATURES

The iDIN can be used as authentication methods in Connective eSignatures. This authentication method goes beyond the most basic signing method (i.e. anything other than "*manual*" signing) as described below:

iDIN	Authentication and identification via the iDIN scheme. Connective eSignatures will receive personal information about the authenticated user via iDIN, at least first name initials, last name, unique iDIN identifier, (out of the KYC of the banks, related back to the Dutch identity card).

When using iDIN as a signing method, the signatory is asked to select the (Dutch) bank with which he or she has an account, and through a dedicated iDIN page on that bank's website is asked to confirm (after logging into the account) that certain data can be shared with Connective eSignatures. That data will include at least first name initials, last name and unique iDIN identifier. Connective eSignatures then embeds information related to the transaction and the identity of the signatory into the signature. The data used for this signing method is arguably **uniquely linked** to the individual (though the limitation in some cases to first name initials limits this to a certain extent). As the signature creation data comes from the information shared by the bank with Connective eSignatures (and as the signatory has to log into his or her account on the bank's website beforehand), one can also argue that this data is under the **sole control** of the signatory (as without logging in to the bank as the signatory and using the proper authentication method, no one else can generate such a signature). This (combined with the two other criteria for an AES, which are more easily established in the case of all Connective eSignatures signing methods) leads us to conclude that the iDIN signing method in Connective eSignatures can be viewed as an **AES**. However, in the absence of any certification, it will not be able to qualify as a QES.

Signing method	SES	AES	QES
iDIN	✓	✓	✗

3.4 Conclusion

Connective eSignatures is a cloud-based electronic signature solution that handles all key aspects of the electronic signature process.

When using Connective eSignatures, the onboarding of signatories remains the responsibility of the initiator of the signing process, except in specific cases that involve onboarding by a third party (e.g. Belgian eID, itsme or iDIN). As a result, when using the other available signing methods, it is up to the initiator to verify the signatory's identification data and contact details, such as name, e-mail address and mobile phone number.

After this identity verification, all other steps are handled by Connective eSignatures directly or through Connective eSignatures with the involvement of a third-party service provider (e.g. for time-stamping), and all individuals listed as signatories follow a procedure that involves various (single- or multi-factor) authentication methods (e.g. one-time passwords, PIN codes for cards, etc).

Moreover, Connective eSignatures has been built in such a way that the process clearly captures the intent of the signatories. Finally, in order to protect the final and signed document against subsequent changes,

Connective eSignatures maintains an audit trail that records any changes made to the signed document and certifies the final document before circulating it to all participants.

With its breadth of signing methods supported, Connective eSignatures allows the initiator of the signing process to choose the settings that are most appropriate to the document in question and intended legal consequences.

Where this is properly done, we conclude with confidence that Connective eSignatures is a tool that allows to produce simple electronic signatures that meet or even exceed the requirements of a (simple) "*electronic signature*" (**SES**) 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.

While such an SES 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, an SES will often be considered as adequate. 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, Connective eSignatures provides important evidentiary value by providing a multi-factor authentication in several cases, registering every single action on Connective eSignatures in all cases and certifying the signed document in each case as well.

Furthermore, depending on the chosen settings and the onboarding procedure implemented in practice (where applicable), these signatures can also meet the requirements for an advanced electronic signature (as defined in Article 3(11) of the eIDAS Regulation - **AES**) or even those of a qualified electronic signature (as defined in Article 3(12) of the eIDAS Regulation - **QES**). Support for such QES solutions means in practice that in accordance with Article 25 of the eIDAS Regulation, certain signatures created through Connective eSignatures have a legal effect equivalent to that of a handwritten signature and are recognised in other EU Member States. Connective eSignatures is then an innovative tool to support and facilitate the process of producing AES and QES.

Finally, Connective eSignatures works with external trust providers to offer reliable means to guarantee the long-term validity of such signatures.

Connective eSignatures is an 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. Connective eSignatures in particular allows users to configure and build workflows in accordance with the user's specific compliance, industry and risk profile.

4. Switzerland

In this chapter, we first give an overview of the relevant electronic signature rules in Switzerland. Then, we reflect on the validity and enforceability of electronic agreements in Switzerland. Finally, we analyse the legal effectiveness of Connective eSignatures in light of the applicable legal framework.

4.1 Electronic signature rules

FAES - The Swiss Federal Act on Electronic Signatures (the **FAES**) regulates the conditions under which service providers may use certification services with electronic signatures. Additionally, the FAES provides a framework outlining the provider's obligations and rights applicable to the provision of certification services. The FAES' tiered structure and standards of legal value are similar to those of European Union's eIDAS Regulation.

The OFAES specifies the provisions of the FAES in more depth. This Annex to the FAES contains further details on the requirements providers have to fulfil in order to get certified. In the FAES regulations, next to the general notion and concept of "*electronic signatures*", there are three additional variants, namely advanced, regulated and qualified electronic signatures.

4.1.1 SIMPLE ELECTRONIC SIGNATURES

Broad definition - A simple electronic signature or **SES** is defined broadly in the FAES. According to Article 2(a) FAES a SES is data in electronic form which is attached to or logically associated with other data in electronic form and which aims at authenticating such data. No reference is made to a specific technology.

Three criteria can be inferred from the definition in the FAES, namely: (i) the existence of data in electronic form, (ii) attached to, or logically associated with, other data in electronic form, and (iii) aiming at authenticating the attached/associated data. The FAES does not further define or explain these criteria, and thus leaves room for interpretation and technical innovation.

Legal effect - According to Article 177 of the Swiss Civil Procedure Code (**CPC**), "*electronic files and the like that are suitable to prove legally significant facts*" can be introduced in litigation as "*physical records*".

Under Swiss procedural law, the courts are free in their appraisal of the evidence presented to them (Article 157 CPC), and there is no preference by law for certain forms of evidence. This means that an electronic signature **cannot be denied legal effect and admissibility** as evidence in legal proceedings solely on the grounds that it has an electronic form or that it does not meet the requirements for qualified electronic signatures. Due to the technical measures implemented in the Connective eSignatures products, it might even be less likely that an opposing party would succeed in giving adequate grounds for disputing the authenticity and thus challenging the evidence presented in court.

However, the fact, that a SES may not be denied legal effect and admissibility as evidence based on certain technical characteristics, does not necessarily mean that it will receive the same legal treatment as a handwritten signature (if it is used to sign a contract).

Furthermore, a contract signed with a SES is only legally valid, if mandatory Swiss law does not prescribe written form for the contract in question and if the parties have not agreed by a pre-existing contractual provision to conclude certain contracts only "*in written form*", without further specifying what counts as "*written form*" (see section 4.2 below).

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.

4.1.2 ADVANCED ELECTRONIC SIGNATURES

Four technology-neutral criteria - An advanced electronic signature or **AES** is defined by Article 2(b) FAES as a SES meeting the following additional requirements: (i) it is uniquely linked to its holder; (ii) it is capable of identifying its holder; (iii) it is created with means which the holder can use under his or her sole control; and (iv) it is linked to the associated data in such a way that any subsequent change in the data is detectable. The definition of an AES is technology neutral.

It should be noted that providers of AES **do not necessarily have to be certified** by an accredited conformity assessment body or use certificates issues by a certified body.

Increased level of trust- The Swiss law does not grant any different legal effect to an AES in comparison to a SES. However, AES are generally considered to be more trustworthy and to have a higher evidential value in legal proceedings.

According to the information available, Connective is today offering (non-qualified) electronic signatures with a qualified timestamp. Adding such a qualified timestamp to a (non-qualified) electronic signature is likely to enhance the security and trustworthiness of the electronic signature and its evidential value in legal proceedings and may contribute to meeting the requirements of an AES.

Although the legal effects of advanced electronic signatures are not different from those for simple electronic signatures, advanced electronic signatures are generally considered to be more trustworthy and to possess a higher evidential value in legal proceedings.

4.1.3 REGULATED ELECTRONIC SIGNATURES

Extensive set of criteria - A regulated electronic signature or "***RES***" is defined by Article 2(c) FAES as an AES that is created by a secure **electronic signature creation device** pursuant to Article 6 FAES and is based on a **regulated certificate**.

Article 2(g) FAES specifies that a regulated certificate means a digital certificate (attestation which links the public key to its owner) issued by a body certified under the FAES and meeting the requirements of Article 7

FAES. Details regarding RES and regulated certificates in particular can be found in Articles 4 *et. seq.* of the OFAES and in the Annex.

A **certified body** is a service provider who provides services in accordance with the requirements set out in the 5th section of the FAES and who is certified by an accredited conformity assessment body. In Switzerland, there are currently only four certified bodies (Swisscom (Schweiz) AG, QuoVadis Trustlink Schweiz AG, SwissSign AG and the Federal Office of Information Technology, Systems and Telecommunication) and one accredited conformity assessment body (KPMG).

Increased level of trust - According to Article 59a CO, the providers of a RES (and QES; see below section 4.1.4) are liable to third parties for any loss or damage suffered as a result of relying on a valid regulated or qualified certificate.

Apart from that, the Swiss law does not grant any different legal effect to an RES in comparison to a SES and AES. However, RES are generally considered to be more trustworthy and to have a higher evidential value in legal proceedings compared to SES and AES.

Only certified bodies can issue a regulated certificate that transform an advanced into a regulated electronic signature. Although the legal effects of regulated electronic signatures are not different from those for simple or advanced electronic signatures, regulated electronic signatures are generally considered to be more trustworthy and to possess a higher evidential value in legal proceedings.

4.1.4 QUALIFIED ELECTRONIC SIGNATURES

Definition - A qualified electronic signature (**QES**) is defined in Article 2(e) FAES as an RES based on an **qualified certificate**.

Article 2(h) in connection with Article 8 FAES specifies that a qualified certificate means a digital certificate issued by a certified body under the FAES and meeting the requirements of Article 8 FAES. In contrast to the regulated certificate, **a qualified certificate can be issued only on behalf of a natural person.**

Equal to a handwritten signature - According to Article 14(2bis) CO, a QES combined with an authenticated time stamp within the meaning of the FAES is deemed equivalent to a handwritten signature, subject to any statutory or contractual provisions to the contrary. This means that a QES is automatically deemed equal to a handwritten signature (wet ink signature) and has the equivalent legal effect. However, a QES may not be sufficient by itself to validly conclude a contract in cases where Swiss law prescribes a qualified written form (such as a certification by a notarial act for real estate transactions; see section 4.2 below).

According to the information available, Connective is partnered up with a qualified trusted service provider (certified body) in Switzerland which would allow Connective to offer QES in Switzerland in the near future.

The certificate that transforms a regulated electronic signature into a qualified electronic signature needs to meet additional requirements. A qualified electronic signature automatically has the equivalent legal effect of a handwritten signature.

4.2 Validity and enforceability of electronic agreements

Swiss contract law does not generally require contracts to be in written form and/or signed. However, certain types of agreements must be in writing in order to be valid.

Swiss law considers digital signatures to be **equivalent to a handwritten signature**, provided the digital signature is based on an authenticated certificate issued by a provider of certification services within the meaning of the FAES.

The use of Connective eSignatures will have the following impact on the validity and enforceability of digitally signed agreements.

Validity - Swiss contract law does, in general, not require the observation of a specific form for contracts. Contracts can be concluded either orally, by implicit action, or by any other means of expressing the parties' intent. A specific form, in particular the written form requiring a wet ink signature, is only required where so expressly prescribed by either (mandatory) law or by a pre-existing contractual provision between the parties.

Mandatory provisions requiring wet ink signatures may primarily be found in B2C relationships, e.g. tenancy law, employment law for apprenticeships, etc. In general, regular B2B contracts are usually not subject to written form requirements, with certain exceptions regarding either specific types of transactions or specific provisions.

Written form is required for example in Article 165 CO (assignment of claims) and mentioned in Article 82 of the Swiss Federal Debt Enforcement and Bankruptcy Act. Further relevant areas where mandatory statutory provisions prescribe the written form including wet ink signatures are real estate transactions and company incorporations. Please note that these are examples only, and not an exhaustive list of mandatory provisions requiring the written form. Swiss law provides for a number of additional mandatory written form requirements that may apply, depending on the scope and content of the contract in question.

According to Article 16(1) CO, the **parties may subject a contract to formal requirements** where such requirements are not prescribed by mandatory law. Article 16(2) CO states that where the parties stipulate a written form without further details, the provisions governing the written form as required by law apply to satisfy such requirement. Under Swiss law, the formal requirement for "*written form*" includes a wet ink signature (Article 14(1) CO).

As a consequence, if the parties have agreed by a pre-existing contractual provision to conclude certain contracts only "*in written form*", without further specifying what may be considered as "*written form*", this would be construed as to require a wet ink signature. This might for example be the case where pre-existing

framework agreements stipulate the written form for contracts, purchase orders or the like concluded under such framework agreement.

If such contracts, purchase orders, etc, are concluded with Connective eSignatures, there is a certain risk that either party may challenge the validity of such contract. However, if both parties make continued use of Connective eSignatures for the conclusion of such contracts, purchase orders, etc, this could then be construed as an implicit agreement to waive the initial written form requirement to include such less stringent form as well, preventing either party to invoke the pre-existing contractual provision.

Since Swiss contract law does, in general, not require the observation of a specific form for contracts, contracts concluded using the Connective eSignatures products are **in principle legally valid**. However, the signing methods provided by Connective eSignatures do not meet the requirements of a QES and the QES is, as already stated above, the only signing method equivalent to a handwritten signature. As a consequence, a contract concluded using the Connective eSignatures products would in an individual case not be legally valid where a contract pertains to a transaction (or contains specific provisions) regarding which mandatory Swiss law prescribes the written form or where the parties have agreed by a pre-existing contractual provision to conclude certain contracts only "*in written*" form. Whether (and if so where) this is the case would have to be assessed on a case-by-case basis taking into account the exact scope and content of the contracts in question.

Enforceability - As mentioned in section 4.1.1 above, electronic files and the like that are suitable to prove legally significant facts can be introduced in litigation as "*physical records*" (Article 177 CPC), the courts are free in their appraisal of the evidence presented to them (Article 157 CPC) and there is no preference by law for certain forms of evidence. Contracts concluded using the Connective eSignature products would thus have the same probative value in litigation as "*wet ink signature*" contracts.

Records introduced as evidence in litigation are rarely disputed, in particular due to the dire consequences of forgery (custodial sentence of up to five years; see Article 251 of the Swiss Criminal Code). The party introducing a record in litigation must prove its authenticity upon the opposing party's giving adequate grounds for disputing its authenticity (Article 178 CPC).

Regarding the probative value in litigation, **the qualification of the product used to sign a contract is not decisive**. Contracts signed using the Connective eSignature products would benefit from the same probative value in court as a contract signed with a QES within the scope of FAES (which would be considered equivalent to a "*written contract*") or an actual contract with wet ink signature. Due to the technical measures implemented in the Connective eSignature products it might even be less likely that an opposing party would succeed in bringing forward adequate grounds for disputing the authenticity and thus challenging the evidence presented in court.

The vast majority of agreements do not require any formalities to be valid. As Swiss courts are free in their appraisal of the evidence presented to them, the qualification of the product used to sign a contract is not decisive.

4.3 Connective eSignatures compliance assessment

This section of the document discusses how the legal requirements for simple, advanced, regulated and qualified electronic signatures (as set out above) apply to Connective eSignatures and which of these requirements are met by Connective eSignatures.

4.3.1 CONNECTIVE ESIGNATURES MEETS THE SWISS REQUIREMENTS OF ELECTRONIC SIGNATURES

Connective eSignatures allows producing SES under Swiss law. All available signing methods (Manual signing, E-mail OTP, SMS OTP, Biometric, iDIN, Belgian eID, Manual + Belgian eID, LawyerID and itsme) consist of data in electronic form which is attached to, or logically associated with, other data in electronic form and which aims at authenticating them and therefore meet the requirements of a SES under Swiss law.

Connective eSignatures allows one to produce simple electronic signatures. In addition, it strives to increase trust and security by (i) allowing advanced identification of the signatories, (ii) capturing the intent to sign in an unambiguous way and (iii) supporting the enforcement of the resulting electronic signature through its audit trail.

4.3.2 NATURE OF SIGNING METHODS SUPPORTED BY CONNECTIVE ESIGNATURES

Based on the information mentioned in the section 4.3.2, we assume that the signing methods "*Biometric*", "*iDIN*", "*Belgian eID*", "*Manual + Belgian eID*", "*LawyerID*" and "*itsme*" are uniquely linked to the holder, are capable of identifying the holder, are created with means which the holder can use under his sole control and are linked to the associated data in such a way that any subsequent change in the data is detectable. Furthermore, as stated in section 4.1.2 above, it is not necessary that the providers of AES are certified by an accredited conformity assessment body in Switzerland or that AES are based on certificates issues by a certified body. As a consequence the mentioned signing methods likely meet the requirements of an AES under Swiss law.

As a general rule, if a signature method is qualified as a QES or AES under the eIDAS regulation, and if the "*signatory*" is the "*holder*" of the signature, then the signature method qualifies as an AES under Swiss law.

None of the by Connective offered signing methods meet the requirements of a RES or QES under Swiss law. Due to the fact Connective eSignatures and the respective providers of the signature methodsare not certified by an accredited conformity assessment body in Switzerland. Also, according to the information available, the signing methods do not include a certificate issued by a body which is certified in Switzerland. However, the signature methods are set-up in that way that Connective could meet these requirements once Connective would decide to request and obtain accreditation or would use local Swiss partners certified by an accredited conformity assessment body in Switzerland for issuing (regulated or qualified) certificates.

The signing methods "*Belgian eID*" and "*Manual + Belgian eID*" are based on a certificate issued by the Belgian government as root certificate authority. "*LawyerID*" features Zetes, and "*itsme*" Belgian Mobile ID

SA/NV as its root certificate authorities. All these authorities are not certified in Switzerland. Foreign providers of certification services which are certified abroad can request the certification in Switzerland. The accredited conformity assessment body in Switzerland (KPMG; see above) can certify them if they meet the requirements. Until now however, no foreign certification service provider has requested a certification in Switzerland. An automatic recognition and certification would require the conclusion of an international agreement between Switzerland and the country where the provider is based. No such agreement exists as of now.

In summary, it is possible for Connective (and the original providers of the electronic signature methods, respectively) to request a certification with the accredited conformity assessment body in Switzerland. Alternatively, Connective can include certificates in its products that are issued by certified bodies in Switzerland. Thereby, the signing methods can qualify as RES or QES under Swiss law (provided that all the security requirements are met, in particular with regard to the secure electronic signature creation device; see section 4.1.3 above). Furthermore, Connective can add signature methods to its platform which are qualified under Swiss law as QES, such as the "*SuisseID*" by SwissSign Ltd., the "*All-in Signing Service*" by Swisscom (Schweiz) Ltd. or the "*QuoVadis Signing Service*" and "*Primo Sign Engine*" by Quovadis Trustlink Schweiz Ltd.

Connective eSignatures allows the use, depending on the choices of the initiator of the signing process (based on the nature of the document and desired legal consequences), of simple, advanced and qualified electronic signatures, in a manner that enables long-term validity of such signatures.

4.4 Conclusion

We conclude that Connective eSignatures is a tool allowing to produce SES meeting or even exceeding the requirements of a SES as defined in Article 2(a) of the FAES. Such signatures may not be denied legal effectiveness solely based on their technical characteristics.

Some of the signature methods (namely "*Biometric*", "*iDIN*", "*Belgian eID*", "*Manual + Belgian eID*", "*LawyerID*" and "*itsme*") likely qualify as AES as defined in Article 2(b) FAES. AES are generally considered more trustworthy than SES and possess a higher evidential value in legal proceedings. Other than that, AES do not grant substantial benefits with regard to validity or effectiveness compared to SES since QES is the only category equivalent to a handwritten signature.

None of the analysed signing methods meets the requirements of a RES or QES (as defined in Article 2(c) and 2(e) FAES) because Connective eSignatures (and the original providers of the analysed signing methods, respectively) are not certified by an accredited conformity assessment body in Switzerland, nor do the signing methods use (regulated or qualified) certificates issued by a body which is certified in Switzerland. However, the signature methods are set-up in that way that Connective could meet these requirements once Connective would decide to request and obtain accreditation or would use local Swiss partners certified by an accredited conformity assessment body in Switzerland for issuing (regulated or qualified) certificates.

The fact that "*Belgian eID*", "*Manual + Belgian eID*", "*LawyerID*" and "*itsme*" qualify as QES under European law does not imply that they are qualified in the same category under Swiss law. The mutual recognition of electronic signatures would require the conclusion of an international agreement. Switzerland has not concluded such an agreement with the EU.

However, as set out in section 4.1.4. above, Connective currently offers (non-qualified) electronic signatures with a qualified timestamp and is partnered up with a certified body in Switzerland which would allow Connective to offer QES in Switzerland in the near future.

5. United States

The first part of this chapter discusses United States' law applicable to electronic signatures and transactions in the U.S. market, specifically the Electronic Signatures in Global and National Commerce Act (**"ESIGN"**) and the Uniform Electronic Transactions Act as approved and recommended by the National Conference of Commissioners on Uniform State Laws in July 1999 (**"UETA"**) (collectively referred to as the "*U.S. eCommerce Laws*").

The second part of this Addendum compares the key functions of Connective eSignatures with the requirements of the U.S. eCommerce Laws to assess whether the electronic signatures produced by Connective eSignatures are legally binding

Note: This analysis is not customized to any particular type of transaction - whether consumer or business-to-business. As certain documents are excluded from coverage by the U.S. eCommerce Laws, and other types of documents must meet different legal requirements to be accepted in electronic form, it is recommended that users of Connective eSignatures verify which settings are most appropriate in light of the nature of the document(s) being executed and desired legal consequences.

5.1 Electronic signature rules

5.1.1 GENERAL STRUCTURE

The United States has a two-tier structure of laws - federal and state. Federal applies to the entire nation and to transactions involving parties of different states; while state laws apply only to the specific state and transactions conducted within that state. With respect to the U.S. eCommerce Laws, Electronic Signatures in Global and National Commerce Act (**ESIGN**) was enacted at the federal level while Uniform Electronic Transactions Act (**UETA**) is enacted at the state level.

While ESIGN and UETA are very similar, there are substantive differences. It is important to consider which law applies to a given transaction. ESIGN affects writing and signing requirements of both state and federal U.S. laws. Federal writing and signature requirements will always be governed by ESIGN. Additionally, ESIGN overrides state law with respect to transactions in or affecting interstate or foreign commerce. Like the eIDAS Regulation, ESIGN is directly applicable to each of the U.S. states and does not need to be adopted by each state with respect to such transactions.

For those transactions that are not affecting interstate or foreign commerce, ESIGN, by its terms, allow states limited authority to modify, limit or supersede ESIGN by adopting either (i) the official text of UETA or (ii) any other law which is consistent with ESIGN and does not require or give preferential status to any specific technology. If a state enacts the official version of UETA, then the UETA provisions may supersede the provisions of ESIGN with respect to state law (but not U.S. federal law). If a state adopts an alternative to UETA, however, that alternative is pre-empted by ESIGN to the extent such alternative is not consistent with ESIGN. Therefore, for most purposes, a cautious approach would assume that ESIGN sets the baseline

rules for those states that have not enacted the official version of UETA. For this reason, both ESIGN and the official version of UETA are discussed in the section below.

ESIGN contains the electronic signature rules for transactions in or affecting interstate or foreign commerce. States can enact the UETA which may supersede the provisions of ESIGN with respect to state law.

5.1.2 ESIGN

Broad definition - ESIGN allows for many possible variants of the concept of "*electronic signature*". ESIGN defines an electronic signature as an "*electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record*". However, unlike the eIDAS Regulation, ESIGN **does not specify exactly what form an electronic signature should take**, but rather allows parties to determine for themselves the technology that is most effective for them and for the transaction at hand. The choices could range from a simple click-through process (e.g. an "*I Agree*" button), to a PIN number (e.g. an SMS OTP), to a single string of numeric code that is encrypted, to electronic scanners that read thumbprints or eye patterns, or any combination thereof. ESIGN also does not address the issue of authentication. It is important to note the use of the term "***process***" in the definition. This means that the creation of an electronic signature under ESIGN may involve multiple steps and consideration of surrounding circumstances. For example, as part of a contract execution, assume that a signatory appears at a business's offices, where his identity is verified by reference to his driver's license and other identification. The signatory is then placed in front of a computer, where he types his name at the end of an electronic form contract intending to signify acceptance of the contract terms, and the business also notes on the form the steps taken to identify the signatory. The entire process, including the verification of identity and the affixing of the typed name to the contract, would constitute a "*process*" resulting in an electronic signature.

Intent - Different from the eIDAS Regulation, the ESIGN definition of an electronic signature also requires that the signatory intend to sign the record, and not only that the signatory use the sound, symbol or process to sign. However, ESIGN does **not address exactly how a signatory must manifest such intent**. Currently, a number of conventions are used with written documents in order to provide evidence of the intent to sign: placement of the signature at the end of the document, statements above the signature that the signatories are signing the document to demonstrate their agreement to the terms in the document, notarized acknowledgments of the signature, etc. Because the requirement of an intention to sign is built into the definition of an electronic signature under both ESIGN and UETA, parties hoping to enforce signed records at a later date should include a certain amount of ceremony as part of the electronic signing process; failing to do so creates the risk of a later claim that there was no intent to sign, and therefore no valid electronic signature.

Electronic record capable of retention - An "*electronic record*" under ESIGN is a record created, generated, sent, communicated, received or stored by electronic means, which record is stored in an electronic medium and retrievable in perceivable form. Essentially, all that is required is that the information be stored in electronic form and may be retrieved for review. The requirement that the electronic record be "***retrievable in perceivable form***" is an objective, and not subjective, requirement. To qualify, it is not

necessary that the specific recipient be able to comprehend the information contained in the record, just that someone could comprehend it. For example, a data file stored on a hard drive which displays information in Spanish is a record for purposes of ESIGN, even if the person reviewing the record cannot read Spanish.

There is a condition to ESIGN's general rule of validity of electronic records. If a contract or other record is required by another U.S. statute, regulation or rule to be made "*in writing*", the legal effect, validity, or enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and capable of being accurately reproduced for later reference by all parties. Thus, **electronic records required to be in writing must be capable of being retained** and accurately reproduced for later reference.

Special protection for consumers - As a general matter, ESIGN does not require any person to agree to use or accept electronic records or signatures. However, consumers receive special protection under ESIGN. "*Consumer*" is defined in ESIGN §7006(1) as "*an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual*". Additionally, there are 17 states that have incorporated the ESIGN consumer protection provisions into the state UETA.

Under ESIGN, electronic records can satisfy any law that requires that records be provided to consumers "*in writing*" only if (i) the consumer is provided with certain disclosures of the hardware and software requirements to access and retain the records (the **ESIGN Consent Disclosures**), including of changes to the hardware or software requirements and (ii) the consumer affirmatively consents to being provided with such electronic records and has not withdrawn such consent (the **ESIGN Consumer Consent Process**). Furthermore, the consumer must consent electronically, or confirm his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent. Consent must be obtained first in order for the "*in writing*" requirements to be deemed to be met. There is little legal or legislative guidance to assist with the interpretation of the reasonable demonstration requirement. However, the **reasonable demonstration requirement** is subjective and fact-based. It requires a "*reasonable*" demonstration, not actual proof. A consumer, conceivably could raise a defense in a dispute relating to required consumer information that he or she was unable to access that information. Therefore, in considering which strategy to use to meet the reasonable demonstration requirement, companies should understand that the closer the reasonable demonstration comes to actually demonstrating the consumer's ability to deploy the chosen technology, questions are less likely to arise later regarding the effectiveness of the particular strategy utilized.

While ESIGN does not provide for any penalties for noncompliance with the ESIGN Consumer Consent Process, failure to comply with the ESIGN Consent Disclosures may result in untimely notice of the underlying information or exposure to significant statutory damages and other remedies associated with the substantive law underlying the transaction. Nonetheless, the legal effectiveness or enforceability of any contract entered into with a consumer is not void if the reasonable demonstration requirement is somehow not met. ESIGN specifically provides that the "*legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with the reasonable demonstration requirement*".

ESIGN also does not impose any type of verification requirement on the part of the record provider to ensure that required consumer information was actually delivered, received, or read - although such a requirement may exist under other law applicable to the transaction. However, the purpose of the ESIGN Consumer Consent Process is to verify at the outset by self-reporting or otherwise that the consumer is capable of accessing required consumer information in the format being used by the provider of the record.

Under ESIGN, an electronic signature is (1) a sound, symbol, or process, (2) attached to or logically associated with a record, and (3) executed or adopted by a person with the intent to sign the record. Consumers receive special protection under ESIGN. If records need to be provided to consumers in writing, consumers should be provided with certain disclosures of the hardware and software requirements to access and retain the records and affirmatively consent to being provided with such electronic records and not have withdrawn such consent.

5.1.3 UETA

UETA is a uniform law that each state of the U.S. may choose to enact, in full or in part, or in modified form, as state law. Forty-seven (47) of the U.S. states have adopted UETA in some form.

Differences between ESIGN and UETA - UETA differs from ESIGN in that it applies only to transactions between parties which have agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct. However, as with ESIGN, UETA provides for the legal validity of electronic signatures and records, and UETA's definitions of the terms "*electronic record*" and "*electronic signature*" are materially similar to those of ESIGN.

Attribution - Unlike ESIGN, UETA includes a provision addressing attribution of electronic records, which governs disputes when one party has relied on an electronically signed record but the apparent signatory of the record disavows it. Under UETA, a signature is attributable to a person if it was the act of the person. The act may be shown in any manner, including a showing of the efficacy of any security procedure (such as a password or PIN) applied to determine the person to which the electronic signature was attributable. Moreover, the effect of an electronic signature attributed to a person is determined by the context and surrounding circumstances at the time it was executed or adopted, including the parties' agreement.

Electronic record capable of retention - Again, similar to ESIGN, UETA's general rule of legal validity is also conditional upon the ability to retain the record, if the record must be provided "*in writing*" under other law. UETA also specifically states that an electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record. Certain state implementations of UETA also adopt the ESIGN Consumer Consent Process and the ESIGN Consent Disclosures for records that must be provided "*in writing*" to consumers. Moreover, even if there is no requirement to deliver or otherwise provide information in writing, if a sender inhibits the ability of

a recipient to store or print an electronic record, that electronic record is not enforceable against the recipient. Thus, the sender must assure that the recipient receives and can retain the information.

UETA differs from ESIGN in that it applies only if parties have agreed to conduct transactions by electronic means. Another additional requirement is that the electronic record is attributable to the signatory, which may be shown in any manner.

5.2 Connective eSignatures compliance assessment

5.2.1 CONNECTIVE ESIGNATURES MEETS THE US ECOMMERCE LAWS' REQUIREMENTS OF AN ELECTRONIC SIGNATURE

Requirements - With respect to the use of electronic signatures, both ESIGN and UETA define an electronic signature as any (1) sound, symbol, or process, (2) attached to or logically associated with a record, and (3) executed or adopted by a person with the intent to sign the record. Neither ESIGN nor UETA specify exactly what form an electronic signature should take, but rather each allows the parties to determine for themselves the technology that is most effective for them and for the transaction at hand.

Connective eSignatures - Connective eSignatures allows the initiator of the signing process to select any of multiple signature types (manual, biometric, email OTP, SMS OTP, etc). Regardless of the signature type or types selected, the signatory will need to activate the click box which states "*I declare that I have read all documents and I agree with the "**Privacy Policy**" and the "**Cookie Policy**"* ", after which a second click box is displayed below which states "*I declare that I have opened and read the "**Terms of use**" and "**ESIGN Consent**", and I agree with their terms*" before clicking the "*Start Signing*" button, and provides the required information for the selected signature type (e.g. the OTP, manual drawn signature, etc).

Doing so causes Connective eSignatures to apply a digital seal to the electronic document (either using the Connective digital certificate or the signatory's personal certificate), binding into the document the information regarding the signatory, the information provided by the signatory to sign, and the signing method used. This approach **clearly amounts to a "*symbol or process*"** within the definition of an electronic signature under each of ESIGN and UETA and meets the requirement that the "*sound, symbol or process*" be attached to or logically associated with the underlying electronic document.

The U.S. eCommerce Laws do not change the existing U.S. common law rules concerning contested signatures and the burden of proof. If the authenticity of an electronic signature is in dispute, the person seeking to enforce the signature will be required to prove that the signature was executed by the person against whom enforcement is sought. This means that when a Connective customer accepts electronic signatures, it will need to be satisfied that the approach it has chosen is sufficiently verifiable and reliable, under the circumstances and for the contemplated purpose, to counterbalance the risk of such a dispute.

Connective eSignatures also may be configured by the initiator to confirm the signatory's intent to sign the electronic document. The signatory receives an email signing invitation inviting the signatory to sign documents and must click the unique URL link in the email to access the documents. Once a signatory is

displayed an electronic document that requires an electronic signature, the signatory must scroll through the entire document before starting the signing process. In the documents, the locations where s/he is supposed to sign are clearly indicated by signature boxes containing the signatory's name. The signatory must then agree that s/he has read all documents and agrees with the ESIGN Consent and the policies provided before clicking the "*Start Signing*" button and providing the required information for the selected signature type - creating his or her own unique electronic signature utilizing the signature method provided by the initiator, and in so doing, the signatory's electronic signature is applied to the first signature field in the electronic document(s). Once the signatory has completed providing such required information to create the initial electronic signature, s/he will move on to the next signature field in the document(s) and repeat this process for each electronic document (and each location within that document) that requires a signature.

Taken together, these affirmative acts— clicking the email URL, agreeing that the signatory has read the documents and accepting the ESIGN Consent, clicking the "*Start Signing*" button, selecting the optional signature method, providing the information to create and apply his or her signature—**demonstrate the signatory's intent to sign** the electronic documents because the process leading up to those actions clearly establishes that those actions will result both in the signatory's signature and the signatory becoming obligated on that document. Connective eSignatures captures these affirmative acts by the signatory both in its audit trail and in the signature field itself. These signatures (and the signed electronic documents) are protected from alteration by application of Connective eSignatures' digital certificate or personal certificate for each individual signer to the signed electronic documents.

Connective eSignatures further allows the signatory **to view the electronic documents in perceivable form during the signing process** in the WYSIWYS user interface, and the signatory may choose to download the unsigned documents for review at any time prior to or during execution. Thus, electronic documents executed on Connective eSignatures would meet the definition of an electronic record under ESIGN and UETA.

Therefore, the electronic signature created using Connective eSignatures, if properly configured, would meet the definition of an electronic signature under the U.S. eCommerce Laws because, taken together, the electronic signature is (1) a sound, symbol, or process, (2) attached to or logically associated with a record, and (3) executed or adopted by a person with the intent to sign the record.

Electronic signatures created using Connective eSignatures, if properly configured, would meet the definition of an electronic signature under the U.S. eCommerce Laws.

5.2.2 CONNECTIVE ESIGNATURES MEETS THE ECOMMERCE LAWS' REQUIREMENTS OF AN ELECTRONIC RECORD CAPABLE OF RETENTION

Requirements - As previously noted, the U.S. eCommerce Laws require that the signatory be able to retain copies of records for future reference. Connective eSignatures displays the electronic documents in the WYSIWYS user interface as rendered images in the signatory's browser or in a mobile application, meaning that the signatory must be able to view the documents clearly in the WYSIWYS web user interface to accomplish the signing process. If the signatory cannot view or access the WYSIWYS web user interface, he

or she could not view the electronic document(s) and could not electronically sign or submit the executed electronic document because the signature areas are indicated within the displayed electronic document. This process reasonably demonstrates the signatory's ability to receive and view electronic documents in the format provided during the signing session.

Computers today (as well as mobile devices) rarely need a dedicated PDF viewer to open or view PDFs because, at a minimum, most mainstream web browsers provide such functionality (and the signatory will need a mainstream web browser to access Connective eSignatures). Even if the signatory's web browser does not support such functionality, many computers come pre-loaded with programs that allow users to open and view PDFs. And if neither of those options is available, Adobe Acrobat Reader is a free application that the signatory can download on his or her computer.

Connective eSignatures - With regard to electronic documents that are signed by a signatory, Connective eSignatures appears to meet these requirements as Connective eSignatures applies a digital seal or signature on the documents with a Connective certificate or personal certificate for each individual signatory after full execution and provides the signatory with multiple methods of retaining the sealed and signed electronic documents. First, Connective eSignatures allows signatories to **download and/or print an electronic copy** of the executed electronic documents in PDF both before signing and after signing at the conclusion of the signing session. Second, the signatory is provided an email once the document is executed with **a link** to download the completed and signed electronic documents in PDF format. Third, the signatory, if s/he is a registered user, can also log on to the **Connective eSignatures portal** to access for print or download the completed and signed electronic documents in PDF format.

Connective eSignatures provides the signatory with multiple methods to retain the sealed and signed electronic documents. Therefore, Connective eSignatures appears to meet the requirements of an electronic record capable of retention.

5.2.3 CONNECTIVE ESIGNATURES MEETS THE UETA ADDITIONAL REQUIREMENTS

5.2.3.1 AGREEMENT TO CONDUCT TRANSACTIONS BY ELECTRONIC MEANS

Requirements - Signatories have a choice as to use or accept electronic records and electronic signatures in place of required writings or handwritten signatures. A general agreement to use electronic records and signatures is a prerequisite to engaging in electronic transactions. The form of an agreement to transact electronically can be either (1) express or (2) implied.

No consumers - To the extent that signatories are not consumers, the signing process employed by Connective eSignatures demonstrate that the signatories have agreed to proceed electronically.

Consumers - To the extent that signatories are consumers, the signing processes employed by Connective eSignatures demonstrate that the signatories **have agreed to accept electronic signatures** and records and have not clicked "*Reject*" to withdraw such consent. For these reasons, Connective eSignatures sufficiently captures a signatory's agreement to utilize electronic signatures and records. It should be noted that the agreement by consumers to proceed electronically depends in large part on the sufficiency of the language of the ESIGN Consent containing the ESIGN Consent Disclosures required by ESIGN and those

state UETA enactments that have adopted the consumer protection requirements of ESIGN. The language of the ESIGN Consent used by Connective or any Connective customer is outside the scope of this White Paper.

5.2.3.2 ATTRIBUTION

Requirements - As discussed above, under UETA, a signature is attributable to a person if it was the act of the person. The act may be shown in any manner, including a showing of the efficacy of any security procedure (such as a password or PIN) applied to determine the person to which the electronic signature was attributable. Moreover, the effect of an electronic signature attributed to a person is determined by the context and surrounding circumstances at the time it was executed or adopted, including the parties' agreement.

Connective eSignatures - Connective eSignatures' system process begins with upload of an electronic document to the secure Connective eSignatures website. Access to the document is permitted to the signatory through a unique URL link delivered to the signatory at the signatory's provided email address, and the signatory must acknowledge that the signatory has read all documents and agree with the ESIGN Consent, before clicking the "*Start Signing*" button and taking all actions required to apply his or her electronic signature. Additionally, the initiator of the signing process may configure Connective eSignatures to require the signatory to choose between different means of electronic signature, such as email or SMS OTP or biometric data or a manual signature, or an electronic identity card, requiring the signatory to provide additional data and information to uniquely attribute the electronic signature to that particular signatory.

Connective eSignatures captures each key step in the signing process both in a secured **audit trail** and in the signature fields themselves. The signature field includes the date and time the document was signed, the signatory information, the signature method information, the signature certificate information, and the legal notice (if applicable). However there still is an additional separate audit trail which includes the date and time a document was uploaded, the date and time the document was signed, information on the signing method used, the name and email address of the signatory who applied the electronic signature, and the signature certificate information. Furthermore, after the document is fully executed and the audit trail updated accordingly, Connective eSignatures generates and stores that electronic document along with its related audit trail.

The above security processes and procedures employed by Connective eSignatures in the creation and execution of electronic documents fairly attribute an electronic signature within one of those electronic documents to the corresponding signatory.

Connective eSignatures captures a signatory's agreement to utilize electronic signatures and records. Connective eSignatures also has processes and procedures in place which allow the attribution of an electronic signature to the corresponding signatory.

5.3 Conclusion

With its breadth of signing methods supported, Connective eSignatures allows the initiator of the signing process to choose the settings that are most appropriate to the electronic document in question and the intended legal consequences. With this properly done, we conclude with a high level of confidence that Connective eSignatures is a tool that, in conjunction with appropriate and legally compliant processes, allows the production of electronic signatures and records with respect to certain transactions, each as defined in the U.S. eCommerce Laws.

6. Hong Kong

In this chapter, we first give an overview of the relevant electronic signature rules in Hong Kong, and we reflect on the validity and enforceability of electronic agreements in Hong Kong. Finally, we analyse the legal effectiveness of Connective eSignatures in light of the applicable legal framework.

6.1 Electronic signature rules

Electronic Transactions Ordinance (Cap. 553) - The Electronic Transactions Ordinance (Cap. 553) (**ETO**) provides the legal framework for the recognition of electronic records, contracts and signatures, granting them the same legal status as their paper counterparts. Two sections in particular address the validity of electronic signatures and contracts: (i) section 6 and (ii) section 17 of the ETO.

On the other hand, the Electronic Transactions (Exclusion) Order (Cap. 553B) (**ETO Exclusions**) specifies the ordinances that are excluded from the application of sections 5 (*governing requirements for writing*), section 6 (*governing electronic signature and digital signatures*), section 7 (*governing the presentation or retention of information in its original form*) and section 8 (*governing the retention of information in electronic record of the ETO because of operational, technological, solemnity, or other reasons*) of the ETO. The Permanent Secretary for Innovation and Technology is responsible for specifying the excluded ordinances (section 11 of the ETO).

The ETO and the ETO Exclusions apply throughout Hong Kong.

Hong Kong is a "*two-tiered*" jurisdiction, meaning that it recognizes two forms of electronic signatures, electronic signatures and digital signatures.

6.1.1 ELECTRONIC SIGNATURES

Definition - An electronic signature (**ES**) means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted for the purpose of authenticating or approving the electronic record (section 2 of the ETO).

Legal effect - Under section 6(1) of ETO, an electronic signature satisfies the requirement (subject to exceptions further explained below), where a rule of law requires the signature of a person (the first mentioned person) on a document, if **none of the contracting parties is a government entity** or any person acting on behalf of a government entity, and if:

- the first mentioned person uses a method to attach the electronic signature to or logically associate the electronic signature with an electronic record for the purpose of identifying himself and indicating his authentication or approval of the information contained in the document in the form of the electronic record;
- having regard to all the relevant circumstances, the method used is reliable, and is appropriate, for the purpose for which the information contained in the document is communicated; and

- the person to whom the signature is to be given consents (including consent that can be reasonably inferred from the conduct) to the use of the method by the first mentioned person.

A government entity means a public officer or a public body (section 2 of the ETO).

*An electronic signature satisfies the requirement, where a rule of law requires the signature of a person on a document, if the such document is **not** entered into with a government entity, subject to certain exceptions.*

6.1.2 DIGITAL SIGNATURES

Definition - A digital signature (**DS**) in relation to an electronic record, means an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine:

- whether the transformation was generated using the private key that corresponds to the signer's public key; and
- whether the initial electronic record has been altered since the transformation was generated (section 2 of the ETO).

Therefore, electronic signature (as defined under ETO) is broader, and covers the more limited definition of digital signature. A digital signature is a specific types of electronic signature.

Legal effect - Under section 6(1A) of ETO, a digital signature satisfies the requirement (subject to exceptions further explained below), where a rule of law requires the signature of a person on a document, if such document is entered into with a government entity or a person acting on behalf of the government entity, and if the digital signature is:

- supported by a recognized certificate;
- generated within the validity of that certificate; and
- used in accordance with the terms of that certificate.

Therefore, a digital signature is **a specific type of electronic signature** under Hong Kong law. A digital signature requires the use of an asymmetric cryptosystem and a hash function to generate the signature. Furthermore, not all types of digital signatures have legal effect in Hong Kong. Instead, to have legal effect, the digital signature is required to be supported by a recognized certificate.

A recognised certificate means a certificate recognised by the Hong Kong government under the procedure under section 22 of the ETO. A company may apply to the Hong Kong government for its certificates (i.e. any record issued by such company to support identity of user of the digital signature) under section 20 of the ETO.

Currently, only Hongkong Post Certification Authority and Digi-Sign Certification Services Limited issue recognized digital certificates. Both recognised certificate authorities are Hong Kong entities.

A digital signature is required for a contract with a government entity to be valid. Furthermore, not all types of digital signatures have legal effect in Hong Kong. Instead, to have legal effect, the digital signature is required to be supported by a recognized certificate. So far only two Hong Kong entities have been recognised to support digital signatures under Hong Kong law.

6.1.3 RESTRICTIONS ON USE OF ELECTRONIC SIGNATURES

Types of documents which cannot be executed electronically, nor signed with an electronic signature - Under Schedules 1 and 2 of the ETO, unless a rule of law expressly says otherwise, the following documents cannot be executed electronically, nor signed with an electronic signature:

- wills, codicils or any other testamentary documents;
- trusts (other than resulting, implied or constructive trusts);
- powers of attorney;
- the making, execution or making and execution of any instrument which is required to be stamped or endorsed under the Stamp Duty Ordinance (Cap. 117) other than a contract note to which an agreement under section 5A of that Ordinance relates;
- Government conditions of grant and Government leases;
- deeds, conveyances or other documents or instruments in writing, judgments, and lis pendens referred to in the Land Registration Ordinance (Cap. 128) by which any parcels of ground tenements or premises in Hong Kong may be affected;
- assignments, mortgages or legal charges within the meaning of the Conveyancing and Property Ordinance (Cap. 219) or any other contract relating to or effecting the disposition of immovable property or an interest in immovable property;
- documents effecting a floating charge referred to in section 2A of the Land Registration Ordinance (Cap. 128);
- oaths and affidavits;
- statutory declarations;
- judgments (in addition to those referred to in section 6 of ETO) or orders of court;
- warrants issued by a court or a magistrate;
- negotiable instruments (but excluding cheques that bear the words "not negotiable");
- proceedings before various courts.

Types of instruments which will not be governed by the ETO - Some other Ordinances may have specific requirements for certain instruments. The ETO Exclusion includes the full list of matters not governed by ETO at https://www.elegislation.gov.hk/hk/cap553B. These include:

- section 5(1) of the Contracts for Employment Outside Hong Kong Ordinance (Cap. 78) - which requires that contracts for employment outside Hong Kong should be in writing; and
- section 67(1) (*form and contents of award*) of the Arbitration Ordinance (Cap. 609) - which governs the form and contents of an arbitral award.

Types of record keeping not governed by the ETO - Some other Ordinances may require or permit the authentication of information by an electronic signature for the purpose of that relevant Ordinance. Further, these other Ordinances may contain an express provision which:

- specifies requirements, procedures or other specifications for that purpose;
- requires the use of a specified service; or
- confers a discretion on a person whether or when to accept electronic records or electronic signatures for that purpose.

In the above case, the ETO will not affect such specific provisions as to electronic records imposed by the other Ordinances (section 14 of the ETO).

General limitation on the effect of the ETO - If the effect of section 6 of the ETO on a requirement in an Ordinance for the signature of a person is such that any other requirement in that Ordinance or a related Ordinance (that is a requirement other than the requirement for the signature of a person) cannot be complied with due to the operation of that section, section 6 of the ETO does not apply to the requirement for the signature of a person (section 16 of the ETO).

6.2 Validity and enforceability of electronic agreements

Next to the question of the legal effectiveness of electronic signatures, questions arise in relation to the validity and enforceability of an electronically signed agreement.

Validity - In general, Hong Kong law only requires the presence of an offer, acceptance, consideration and intention to create legal relations in order to make a contract enforceable, unless the contract or a rule of law requires signature of a person on a document. There is no rule of law that requires any of the mentioned types of agreements to be signed in order to be enforceable.

Agreements with non-government entities - In relation to an agreement entered into with non-government entities, so long as that agreement is not excluded from coverage of the ETO (see above for the list of such agreements), then it can be entered into electronically in Hong Kong.

Under section 6(1) of the ETO, if a rule of law requires a signature of a person (the First Mentioned Person), or provides for certain consequences if the First Mentioned Person does not sign the document, an electronic signature satisfies the signature requirement if:

- the First Mentioned Person uses a method to attach the electronic signature to or logically associate the electronic signature with an electronic record for the purpose of identifying himself and indicating his

authentication or approval of the information contained in the document in the form of the electronic record;

- having regard to all the relevant circumstances, the method used is reliable, and is appropriate, for the purpose for which the information contained in the document is communicated; and
- the person to whom the signature is to be given consents to the use of the method by the First Mentioned Person.

Agreements with government entities - Under section 6(1A) of the ETO, where the rule of law requires a signature of a person, or provides for certain consequences if the document is not signed by the person, and the transaction involves a government entity, then the person may only use a digital signature that is:

- supported by a recognized certificate;
- generated within the validity of that certificate; and
- used in accordance with the terms of that certificate.

Simple electronic signatures may not be used in such situations.

Currently, only Hongkong Post Certification Authority and Digi-Sign Certification Services Limited issue recognized digital certificates.

Electronic signatures are commonly used to form agreements between non-government entities (subject to exceptions such as agreements related to land). Digital signatures supported by recognised certificates are required to sign agreements with a government entity.

6.3 Connective eSignatures compliance assessment

6.3.1 CONNECTIVE ESIGNATURES MEETS HONG KONG REQUIREMENTS OF ELECTRONIC SIGNATURES

Connective eSignatures - Based on the above description of Connective eSignatures, Connective eSignatures **meets requirements** for an electronic signature:

- *'letters, characters, numbers or other symbols in digital form*' - electronic signatures created with Connective eSignatures indeed consist of a string of data in digital form;
- *'attached to or logically associated with other electronic record'* - the electronic signature can be attached by the signatory to a variety of electronic documents, whereby Connective eSignatures allows uploading multiple source document formats;
- *'executed or adopted for the purpose of authenticating or approving the electronic record*';

- *'having regard to all the relevant circumstances, the method used is reliable, and is appropriate'* - Connective eSignatures 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 your document or package with name* [Name of the document or package]", with the following wording before the hyperlink to Connective eSignatures: "*Please* click *on the link below to sign your document or package* [Name of the document or package]";
  - when the signatory reviews the document, he is requested to sign the document (the exact method - creating a "*handwritten*" signature on screen, e-mail confirmation, etc, depends on the signing method). The placeholder for that signature is a form field in the document entitled "*Your signature here* [name]";
  - clicking that field brings up a popup screen stating that "*To start the signing process: read and scroll through all documents, declare that you have read all documents and click "Start signing" at the bottom of the page.*";
  - in order to sign a document, the signatory must therefore first scroll through the entire document, tick a box stating "*I declare that I have read all documents and shall comply with the following policies*" and then click on a button stating "*Start signing*";
  - the signatory is then guided through the signature process that applies to the relevant signing method, typically in two stages under the signatory's control (e.g. inputting the signatory's e-mail address for e-mail OTP signing, then submitting the OTP sent by e-mail) followed by a final stage without signatory involvement, namely the integration of the signature within the document;
  - Connective eSignatures only considers the document to have been signed by that signatory once these three stages have been completed. Connective eSignatures then informs the initiator of the signing process of the fact that the signatory has signed the document;
- *'the person to whom the signature is to be given consents to the use of the method by the first mentioned person'* - it can be said that the user, by agreeing to use Connective eSignatures, indicates by conduct its consent to use of electronic signature to the transactions. Under the ETO, consents includes consent that can be reasonably inferred from the conduct.

Types of agreements which can be validly executed by Connective eSignatures

As a result, under section 6(1) of the ETO, an electronic signature produced with Connective eSignatures on a document can, in principle, not be denied legal effect, unless:

- such document is signed with a government entity or a person acting on behalf of a government entity; and/or
- such document is an exempted document or instrument as explained above. Please see section 6.1.3 for:
  - types of documents which cannot be executed electronically, nor signed with an electronic signature; and
  - types of instruments which will not be governed by the ETO.

Connective eSignatures ***meets the requirements*** *for an electronic signature.*

6.3.2 CONNECTIVE ESIGNATURES AND THE REQUIREMENTS FOR SIGNING USING DIGITAL SIGNATURES

Connective eSignatures - Based on the above description of Connective eSignatures, Connective eSignatures **do not meets requirements** for a digital signature, as **Connective is not a recognised certification authority in Hong Kong. However, these requirements could be met when using a recognized certification authority in Hong Kong for issuing signatures.**

- *'electronic signature of the signer'* - as above, Connective eSignatures produce electronic signatures which meet the requirements for an electronic signature as defined under the ETO;
- *'generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function'* - Connective's certificate for Connective eSignatures is cryptographically bound during the signing process to the document using the private key held by Connective, in order to preserve the integrity of the document. Connective eSignatures can meet this requirement if a hash function is used to generate the electronic signature;
- *'a person having the initial untransformed electronic record and the signer's public key can determine: whether the transformation was generated using the private key that corresponds to the signer's public key; and whether the initial electronic record has been altered since the transformation was generated'* - we understand that Connective eSignatures is cryptographically bound during the signing process to the document using the private key held by Connective, in order to preserve the integrity of the document;
- *'digital signature is supported by a recognized certificate, generated within the validity of that certificate; and used in accordance with the terms of that certificate'* - Connective eSignatures do not meet this requirement, as it is not a recognised certification authority under the ETO. *Foreign companies can become recognised certification authorities under the ETO and issue certificates for digital signatures, provided they satisfy the requirements which are set out in greater detail in the application form. Currently, only Hongkong Post Certification Authority and Digi Sign Certification Services Limited issue recognized digital certificates. Both recognised certificate authorities are Hong Kong entities.* Currently, only Hongkong Post Certification Authority and Digi-Sign Certification Services Limited issues recognized digital certificates. Both recognised certificate authorities are Hong Kong entities.

Connective eSignatures do not meet the requirements for a digital signature, mostly as Connective is not a recognised certification authority in Hong Kong. This is due to change if Connective would request and obtain accreditation to become a recognized certification authority.

6.3.3 NATURE OF SIGNING METHODS SUPPORTED BY CONNECTIVE ESIGNATURES

Different signing methods, different classification - As described previously, the ETO makes a distinction between general **electronic** signatures and **digital** signatures.

By way of a reminder:

- as indicated above, Connective eSignatures meets **most requirements** for an electronic signature;

- a **digital** signature means an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine:
  - whether the transformation was generated using the private key that corresponds to the signer's public key; and
  - whether the initial electronic record has been altered since the transformation was generated.

Furthermore, to validly use a digital signature, the digital signature should be:

- supported by a recognized certificate;
- generated within the validity of that certificate; and
- used in accordance with the terms of that certificate.

Connective eSignatures do not meet the requirements for digital signatures under ETO, as Connective is not a recognised certification authority in Hong Kong.

6.4 Conclusion

Connective eSignatures is a cloud-based electronic signature solution that handles all key aspects of the electronic signature process.

When using Connective eSignatures, the onboarding of signatories remains the responsibility of the initiator of the signing process. As a result, when using the other available signing methods, it is up to the initiator to verify the signatory's identification data and contact details, such as name, e-mail address and mobile phone number.

After this identity verification, all other steps are handled by Connective eSignatures directly or through Connective eSignatures with the involvement of a third-party service provider (e.g. for time-stamping), and all individuals listed as signatories follow a procedure that involves various (single- or multi-factor) authentication methods (e.g. one-time passwords, PIN codes for cards, etc).

Moreover, Connective eSignatures has been built in such a way that the process clearly captures the intent of the signatories. Finally, in order to protect the final and signed document against subsequent changes, Connective eSignatures maintains an audit trail that records any changes made to the signed document and certifies the final document before circulating it to all participants.

Finally, Connective eSignatures works with external trust providers to offer reliable means to guarantee the long-term validity of such signatures.

As above, Connective eSignatures **meets requirements** for an electronic signature. As a result, an electronic signature produced with Connective eSignatures on a document can, in principle, not be denied legal effect, **unless** (i) such document is signed with a **government** entity or a person acting on behalf of a

government entity; and/or (ii) such document is an **exempted** document or instrument as explained above. (cfr. section 6.1.3).

*Connective eSignatures **meets requirements** for an electronic signature. As a result, an electronic signature produced with Connective eSignatures on a document can, in principle, not be denied legal effect, save for certain exempted documents which cannot be signed electronically.*

7. Singapore

The first part of this chapter discusses Singapore's law applicable to electronic signatures (the Electronic Transactions Act (Cap. 88) (**"ETA"**)). The second part of this chapter assesses how the Connective eSignatures regime meets (or does not meet) the requirements of the ETA.

7.1 Electronic signature rules

7.1.1 BACKGROUND

The ETA is legislation that provides for the security and use of electronic transactions in Singapore. The ETA was first enacted in July 1998 to provide a legal foundation for electronic signatures, and to give predictability and certainty to contracts formed electronically. The ETA provides for the legal recognition and use of electronic signatures and electronic records, thereby providing certainty to electronic transactions.

The ETA has four key purposes:

1. to remove legal uncertainties over electronic writing and signature requirements;
2. to provide a Public Key Infrastructure for digital signatures;
3. use and acceptance of electronic documents by public agencies; and
4. liability of network providers in Singapore for third party content.

Further, the ETA is underpinned by three principles:

1. **Non-discrimination** - An electronic document should not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form.
2. **Functional equivalence** - Electronic records or communications are treated as fulfilling a traditional paper-based requirement if specified conditions are met.
3. **Technological neutrality** - Provisions are drafted to be neutral with respect to the technology used.

The ETA applies throughout Singapore.

Singapore is a "*two-tiered*" jurisdiction, meaning that it recognises two forms of electronic signatures, simple electronic signatures and secure electronic signatures.

7.1.2 SIMPLE ELECTRONIC SIGNATURES

Legal requirement for signature - Section 8 ETA sets out the legal framework governing electronic signatures. In brief, where a rule of law requires a signature, or provides for certain consequences if a document or record is not signed, that requirement is satisfied in relation to an electronic record if:

- a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record; and

- the method used is either:
  - as reliable as appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
  - proven in fact to have fulfilled the functions described in the first bulletpoint above, by itself or together with further evidence.

Section 2(1) of the ETA defines "*electronic record*" as "*a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another*".

Section 6 ETA gives legal recognition to electronic records by declaring the following:

"*For the avoidance of doubt, it is declared that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.*"

An electronic signature satisfies the requirement, where a rule of law requires the signature of a person on a document, if certain conditions are met in in respect of the method used to electronically sign the document.

7.1.3 SECURE ELECTRONIC SIGNATURES

Section 18(1) of the ETA provides that an electronic signature that has been properly **verified by either specified security procedures** or **commercially reasonable security procedures** will be treated as a secure electronic signature. A secure electronic signature is **a specific type of electronic signature** under Singapore law. In order for an electronic signature to be considered a secure electronic signature, it must meet certain requirements which we shall elaborate on below.

An electronic signature will be a secure electronic signature if it is able to meet the following requirements at the time that it was made - the signature was:

- unique to the person using it;
- capable of identifying such person;
- created in a manner or using a means under the sole control of the person using it; and
- linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated.

The "*specified security procedures*" which a secure electronic signature must meet are specific procedures relating to digital signatures. These are determined by the Minister and set out in the Second Schedule of the ETA. Digital signatures require transformation of an electronic record using an asymmetric cryptosystem and a hash function such that the person having the initial untransformed electronic record and the signer's public key can accurately determine:

- whether the transformation was created using the private key that corresponds to the signer's public key; and

- whether the initial electronic record has been altered since the transformation was made (section 1(a), Third Schedule, ETA).

To elaborate on these requirements, a digital signature satisfies the requirement, where a rule of law requires the signature of a person on a document, if the digital signature is:

- created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and
- the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because:
  - the certificate was issued by an accredited certification authority operating in compliance with the regulations made under section 22 of the ETA;
  - the certificate was issued by a recognised certification authority;
  - the certificate was issued by a public agency approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or
  - the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

An "*accredited certification authority*" means a certification authority accredited by the Controller pursuant to any regulations made under section 22 of the ETA. *Foreign companies can become accredited certification authorities under the ETA in Singapore. However, they must satisfy the requirements which are set out in greater detail in the application form and the Electronic Transactions (Certification Authority) Regulations 2010 issued under the ETA, including being a company operating in Singapore at the time of the application and throughout the period when it is an accredited certification authority. Companies may apply to the Singapore Government to be a certification authority. Currently, only Netrust Pte Ltd has been licensed as an accredited certification authority.*

In respect of the other type of secure electronic signatures, in order to determine what is "*commercially reasonable*", regard shall be had to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including:

- the nature of the transaction;
- the sophistication of the parties;
- the volume of similar transactions engaged in by either or all parties;
- the availability of alternatives offered to but rejected by any party;
- the cost of alternative procedures; and
- the procedures in general use for similar types of transactions.

Two types of secure electronic signature are valid in Singapore - those which meet "specified security procedures" (these secure electronic signatures will be

considered "digital signatures") and those which meet "commercially reasonable procedures".

7.1.4 EXCEPTIONS

The First Schedule of the ETA provides that Part II of the ETA (relating to electronic records, electronic signatures and electronic contracts) shall not apply to any rule of law requiring writing or signatures in the following matters:

- the creation or execution of a will;
- negotiable instruments, documents of title, bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money;
- the creation, performance or enforcement of an indenture, declaration of trust or power of attorney, with the exception of implied, constructive and resulting trusts;
- any contract for the sale or other disposition of immovable property, or any interest in such property; and
- the conveyance of immovable property or the transfer of any interest in immovable property.

7.2 Connective eSignatures compliance assessment

7.2.1 CONNECTIVE ESIGNATURES MEETS THE SINGAPORE LEGAL REQUIREMENTS OF AN ELECTRONIC SIGNATURE

Connective eSignatures - Connective eSignatures allows real-time visibility on when a document was uploaded, when it was signed, which signing method was used, the status of the signature process, the list of all signers and the list of all receivers. Each (key) step in the signing process is also captured in an audit trail that is secured and that provides evidence in a clear format, easily produced, of each signatory's signature. This audit trail is by default only available to the administrator. This meets the requirements of "***able to identify the person***".

Connective eSignatures also may be configured by the initiator to confirm the signatory's intent to sign the electronic document. The signatory receives an email signing invitation inviting the signatory to sign documents and must click the unique URL link in the email to access the documents. Once a signatory is displayed an electronic document that requires an electronic signature, the signatory must scroll through the entire document before starting the signing process. Taken together, these affirmative acts demonstrate the signatory's intent to sign the electronic documents because the process leading up to those actions clearly establishes that those actions will result both in the signatory's signature and the signatory becoming obligated on that document. This meets the requirements of ***"able to identify the person's intent in respect of the information contained in the electronic record***".

Finally the three stage authentication process that occurs when using any of multiple signature types (manual, biometric, email OTP, SMS OTP, etc) will, depending on the type of transaction, satisfy the requirements of "***reliable as appropriate or fulfils the necessary functions***".

Therefore, the electronic signature created using Connective eSignatures, if properly configured, would meet the definition of an electronic signature under the ETA.

*Connective eSignatures **meets the requirements** for an electronic signature.*

7.2.2 CONNECTIVE ESIGNATURES MEETS THE SINGAPORE LEGAL REQUIREMENTS OF A SECURE ELECTRONIC SIGNATURE

Commercially reasonable security procedures - Authentication of Connective eSignatures is a two and sometimes three step process. The initiator of the signing process has to provide information on each signatory to allow Connective to send that user a notification that a document is available for signature. Connective eSignatures verifies the signatory's identity by sending a unique URL to a signatory. As 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. After having clicked on said URL link, signatories can create a facsimile of a handwritten signature on screen (e.g. using a mouse, stylus or their finger) and click a button (displaying "*sign*") to sign. The third stage of authentication occurs when using any of multiple signature types (manual, biometric, email OTP, SMS OTP, etc). This three step authentication process should be sufficient to satisfy the requirements of "*unique to the person using it*", "*capable of identifying such person*", and "*created in a manner or using a means under the sole control of the person using it*".

For the Belgian eID and LawyerID signing methods, the signatory's certificate is cryptographically bound during the signing process 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. For all other signing methods, Connective's certificate is cryptographically bound during the signing process to the document using the private key held by Connective, in order to preserve the integrity of the document. As long as these methods ensure that if the record was changed the electronic signature would be invalidated, this should be sufficient to satisfy step "*linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated*".

Therefore, the secure electronic signature created using Connective eSignatures, if properly configured, would **meet the definition of a secure electronic signature** implementing commercially reasonable procedures under the ETA.

Digital signatures - The secure electronic signature created using Connective eSignatures would not meet the definition of a digital signature as it is not an accredited certification authority under the ETA. Currently, only Netrust Pte Ltd is an accredited certification authority.

Connective eSignatures does meet the requirements for a secure electronic signature. However, as Connective is not an accredited certification authority in Singapore, it does not meet the requirements for digital signature under the ETA.

However these requirements could be met when using a recognized certification authority in Singapore for issuing signatures.

7.3 Conclusion

Connective eSignatures allows the initiator of the signing process and their intention to be identified. The method used is as reliable as appropriate and fulfils the necessary function of an electronic signature. For secure electronic signatures, at the time the electronic signature is made it is unique to the person using it and Connective eSignatures is capable of identifying such person. Further, the electronic signatures are created in a manner or using a means under the sole control of the person using it; and it can be linked to the electronic record in which if the record was changed the electronic signature would be invalidated.

There is a legal presumption that a secure electronic record has not been altered since the specific point in time to which the secure status relates, unless evidence to the contrary is adduced. Therefore with the exception of those matters that are excluded under the ETA, we conclude that Connective eSignatures is a tool that, in conjunction with appropriate and legally compliant processes, allows the production of electronic signatures and secure electronic signatures as defined in the ETA. However, as mentioned above, Connective eSignatures does not meet the requirements for digital signatures under the ETA.

8. About the authors

8.1 Chapter European Union

Prof. dr. **Patrick Van Eecke** is a partner in the IT law Department of DLA Piper in Brussels. He 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), and 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 and the Catholic University of Louvain, teaching European Electronic Business 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.

8.2 Chapter Switzerland

Roland Mathys is partner with Schellenberg Wittmer and head of the firm's technology and data law practice team. Roland has a double degree in computer science and law and earned an LL.M. in information technology law from the London School of Economics (LSE). He is ranked as a leading lawyer by Chambers and Legal 500 and has been singled out as a Thought Leader in data matters by Who's Who Legal.

Floriane Zollinger-Löw is an associate in Roland's team. Floriane is a senior lawyer with a strong background technology and digital matters, particularly from her previous assignment as general counsel of a technology service provider. Both authors have extensive experience in technology related transactions

and advisory matters, including data protection and cybersecurity matters, digitalization, and new technologies.

8.3 Chapter United States

Margo H.K. Tank and **David Whitaker** focus their practice on Digital Transformation Strategy as part of DLA Piper LLP's (US) Intellectual Property and Technology Practice (IPT). Margo also serves as the US Co-Chair of the DLA Financial Services Sector and Co-Chair of the Blockchain and Digital Assets group. Together they have over four decades of experience advising commercial enterprises, including financial service providers, FinTech companies, and technology service providers on the full spectrum of regulatory compliance matters related to the use of electronic signatures, electronic records, identity management, virtual currency and other digital assets to enable fully digital transactions. Margo and David were ranked by Chambers Fintech in 2019. **Liz McClure**, also an attorney in the IPT Practice focusing on Digital Transaction Strategy, assisted with the development of this whitepaper.

8.4 Chapter Hong Kong

Scott Thiel is a partner with DLA Piper Hong Kong's IPT team. Scott's background in engineering and dual qualifications in both intellectual property law and computer science provide him with a unique opportunity to understand the technical aspects of client's ICT and outsourcing projects. He advises both users and suppliers of IT outsourcing services on all aspects of the procurement process. He also advises on complex technology transactions. His work usually involves him on business critical projects frequently valued in the tens or hundreds of millions of dollars. He advises clients across a range of sectors including technology, banking, transport, energy and sport. Scott is ranked as a leading individual in the area of TMT - China (International Firms).

Frankie Tam is a senior associate with DLA Piper Hong Kong's IPT team. Frankie is an international technology lawyer qualified in Hong Kong, New York, and England & Wales. Her practice covers a wide array of commercial and tech-related matters, including significant technology outsourcing transactions, Fintech, Regtech and blockchain services agreements and data privacy matters.

8.5 Chapter Singapore

Yue Lin Lee is a registered foreign lawyer (Singapore) with DLA Piper Hong Kong's IPT team. She focuses her practice on intellectual property and TMT matters, with an interest and experience in a broad spectrum of areas in these fields, including technology-related matters, data protection, and media work throughout Southeast Asia (particularly in Singapore).

www.dlapiper.com