CLE PROGRAM

WHAT’S INK GOT TO DO WITH IT: ENFORCEABILITY OF ELECTRONIC AND TECHNOLOGY-BASED COMMERCIAL LOAN DOCUMENTATION

Sponsoring Committee: Uniform Commercial Code

Co-sponsoring Committees: Commercial Finance, Cyberspace Law, International Business Law

Program Chairs:

Linda Filardi, Capital One Bank, Senior Director and Associate General Counsel
Kiriakoula Hatzikiriakos, Senior Manager, Legal Department, National Bank of Canada

Moderator:

Kiriakoula Hatzikiriakos, National Bank of Canada, Senior Manager, Legal Department,

Panelists:

Linda Filardi, Capital One Bank, Senior Director and Associate General Counsel, New York
Elizabeth Leckie, Allen & Overy, New York
Charles Morgan, McCarthy Tétrault, Montreal
Tracy M. Springer, HSBC, Senior In-house Finance Attorney; Expertise in Legal Innovation and Legal Operations; Strategic Partner to Business, New York
Steve Weise, Proskauer, Los Angeles

Abstract:
In our digitally connected world, parties want to benefit from easy, efficient and convenient ways to transact. The physical closings where all contracting parties with their counsel gather around a table covered with multiple copies of agreements have been replaced in great part with online
exchanges of signed documents. This is particularly true in cross-border transactions where parties are located in various jurisdictions.

Electronic contracting can take various forms, such as exchanging signature pages of a contract through scan and email or accessing a contract through a web-based application that allows the signatory party to sign electronically as directed by the platform. Email exchanges between two parties on contract terms can also result in the formation of a contract.

While using technology to facilitate transactions seems relatively easy, it does present legal and practical challenges. Many countries have established legislation dealing with the use, validity and legality of electronic signatures. Such laws are generally permissive as to the use of electronic methods for executing a contract. For example, in the United States, the Uniform Electronic Transactions Act (UEAT) and the federal Electronic Signatures in Global and National Commerce Act (ESIGN) are “enabling statutes that place electronic records and signatures on a legal par with their paper and ink counterparts”.1

In Canada, all provinces and territories have adopted e-commerce legislation. An electronic signature is valid and enforceable so long as the electronic signature is reliable for the purpose of identifying the person and the association of the electronic signature with the relevant electronic document is reliable.

In Europe, the Regulation (EU) No 910/2014 (the eIDAS Regulation) applies to EU Member States from 1 July, 2016 and “establishes an EU-wide legal framework for electronic signatures (as well as for electronic seals, electronic time stamps, electronic registered delivery services and website authentication).”2 Articles 25(2) and (3) of the eIDAS Regulation “provide that a qualified electronic signature shall have the equivalent legal effect of a handwritten signature

---

1 Juliet M. Moringiello & Steve Weise, Electronic Contracts and E-Signatures, July 2019 (powerpoint), p. 5 (see Annex A of this paper).

and that a qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.”

In the United Kingdom, the “Electronic Communications Act 2000 (the ECA 2000) provides a statutory framework for the admissibility of electronic signatures in England and Wales. Section 7(1) of the ECA 2000 provides that in any legal proceedings (a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and (b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity or integrity of the communication or data. Although the ECA 2000 deals with the admissibility of electronic signatures, it does not deal with the validity of electronic signatures.”

Beyond the general principles of admissibility of electronic signatures for agreements, there can be statutory exclusions in the sphere of commercial transactions – and those are not necessarily the same from one jurisdiction to the another. In the United States, for example, the UETA and E-Sign do not apply to the Uniform Commercial Code (except for articles 2 and 2A). The definition of “signing” under article 1 and “authenticate” under article 9 “anticipate the use of electronic signatures”. Note however that article 3 requires a writing, so electronic signatures on promissory notes in a commercial loan transaction would not be possible.

In Canada, the law can differ from one province to another. For example, in Alberta, a guarantee given by an individual by written agreement must be signed before a lawyer, the guarantor acknowledging the guarantee obligation and signing a certificate in the prescribed statutory form. The same process applies in Saskatchewan for a guarantee relating to farmland or other assets in farming. Given the statutory requirements in these provinces, e-signature solutions cannot be used for such types of guarantees.

Beyond creating valid agreements signed and exchanged via email or using an e-signature process, ensuring their enforceability and non-repudiation in a litigious context brings into play evidentiary principles. How does one preserve the integrity and authenticity of the agreement so as to make it admissible in court proceedings? Is it sufficient to simply exchange scanned copies

---

3 Ibid.
4 Ibid.
5 Juliet M. Moringiello & Steve Weise, Electronic Contracts and E-Signatures, July 2019 (powerpoint), see fn. 1 above, p. 10.
6 Ibid.
of agreements signed in “wet ink” via email? How can the lender prove that the party who signed the loan agreement was in fact the authorized representative of the borrower? The rules of the different jurisdictions relating to a transaction must be examined.

Another important practical consideration is for legal counsel working with financial institutions to understand their client’s internal processes and help them develop best practices for mitigating the various risks throughout the life cycle of a document, from creation to destruction.

**Agenda:**
Examine the legal and practical issues relating to the validity and enforceability of electronic and technology-based commercial loan documentation and apply them through a fictitious fact pattern with cross-border elements.

I. **General Legal and Practical Issues**

For any transaction with cross-border elements:
- seek local advice early;
- basic questions to consider will be broadly similar from one jurisdiction to another;
- basic questions should be raised for jurisdiction of governing law and jurisdiction of any foreign counterparty:
  - Is e-signature enforceable?
  - If yes, does e-signature have the same legal effect as wet ink signature?
  - Are there any particular technical or authentication requirements or formalities?
  - What documents are excluded under law?
- practical considerations may be as important as legal considerations;
- issues may be too complicated to consider in the middle of a transaction or to be cost effective:
○ concepts may differ from one jurisdiction to another i.e. “electronic record”, “electronic” transaction, between wet ink, scanned and “electronic signature”; e-signature process:
  ▪ local guidance may be unclear or still evolving;
  ▪ even if e-signatures are valid, a market practice may not yet have evolved;
  ▪ Are all e-signature software/platforms acceptable?
  ▪ Execution monitoring at closings when e-signature is acceptable for some, but not all documents;
  ▪ UK - July 2016 guidance note prepared by a joint working party of the Law Society and the City of London Law Society⁷ is a good example of consensus building

○ consider more than just the governing law of the agreement:
  ▪ capacity and authority of any foreign counterparties;
  ▪ type of agreement:
    ▪ even if generally valid, e-signatures may not be appropriate for all types of documents e.g. signing formalities or registration/filing requirements to take into account
  ▪ be watchful for other potential nexus with another jurisdiction:
    ▪ e.g. location of documents, place of execution;
    ▪ anticipation of enforcement issues or local litigation considerations;
    ▪ tax, regulatory or record-keeping implications

II. **Case study**

TechyIQ US, a predictive analytics company for the advertising industry based in New York is looking for financing to develop additional AI tools and expand its operations.

TechyIQ US has a Canadian wholly owned subsidiary (registered office in Toronto), TechyIQ Cda. and a UK-based subsidiary, TechyIQ Eng. The property of each of TechyIQ US, TechyIQ

---

⁷ See note 2 above.
Cda. and TechyIQ Eng. consists of real and personal property (such as equipment, intellectual property, receivables, contracts, license agreements, investment property, etc.).

Most of TechyIQ US’s transactions with its clients are digitally concluded either through exchanges of scanned contracts, [emails] and digital signatures. TechyIQ US approaches New York-based ForwardBank for financing. TechyIQ US is looking to have all credit and security documentation signed and executed quickly using “electronic” methods.

ForwardBank analyzes TechyIQ’s financing needs and agrees to extend secured credit facilities to TechyIQ. Forward Bank requires the following:

- credit agreement and promissory note for a 25 million US dollar revolving credit and a 3 million dollar hedging facility;
- security/mortgages on all real and personal property of TechyIQ US, TechyIQ Cda. and TechyIQ UK;
- guarantees from TechyIQ Cda. and TechyIQ UK;
- pledge of equity interests in subsidiaries and other investments held by each TechyIQ entity;
- assignment of key man life insurance policies (from each of the entities);
- certificates of incumbency (with copies of resolutions);
- intercreditor agreement with AI123Bank.

You are counsel to ForwardBank and are being mandated to assist it in understanding the following issues in order to implement an electronically based loan closing process for the TechyIQ US transaction, which it can use for subsequent credit transactions as well. ForwardBank asks you to opine on the following issues:

- Validity and enforceability of pdf-signed and electronically signed loan documents in Canada, US and in the UK;
  - How to ensure integrity and authenticity for evidentiary purposes?
- Legal (i.e. statute restrictions) and operational risks (i.e. document integrity, fraud):
  - Risks relating to authenticity, integrity: fraud and risk of repudiation; how they can arise and how to mitigate;
- Type of credit or security documentation: can all documents in the fact pattern be signed through pdf or e-signed process? Are there legal restrictions based on the type of document involved?
- What policies, best practices or processes should ForwardBank implement? i.e. record management system, maintaining integrity post-closing?
  - Best practices for mitigating the risks.

TechyIQ US is looking to expand in other jurisdictions, such as in Asia (Hong Kong, Singapore), in Germany, the Netherlands, Luxembourg, Australia and Mexico. TechyIQ US will be forming subsidiaries in these jurisdictions. ForwardBank wants to understand the laws and practice in these jurisdictions with a view of requiring guarantees and security from TechyIQ US. Are the legal and practical issues like the ones in Canada, the US and the UK? If not, how do they differ?
  - High level discussion of approaches in various jurisdictions: UK, Germany, Netherlands, Luxembourg, Hong Kong, Singapore, Australia, Mexico
LIST OF REFERENCES (see Annex A below)

- Charles Morgan, McCarthy, *e-signatures and Scanned Documents*, July 2019
ANNEX A: MATERIALS

[materials are separated by a blank page between each source]
Global Guide to Electronic Signature Law:
Country by country summaries of law and enforceability
Table of contents

Introduction 3
Definition of terms 4
Recommended practices for electronic agreements 4

Country summaries of electronic signature law 5
Argentina 5
Australia 5
Austria 9
Belgium 9
Bermuda 6
Brazil 6
Bulgaria 9
Canada 7
Chile 7
China 8
Colombia 8
Croatia 9
Czech Republic 9
Denmark 9
Estonia 9
Finland 9
France 9
Germany 9
Greece 9
Hong Kong 10
Hungary 9
India 10
Indonesia 11
Ireland 9
Israel 11
Italy 9
Japan 12
Latvia 9
Lithuania 9
Luxembourg 9
Malaysia 12
Malta 9
Mexico 13
Netherlands 9
New Zealand 13
Norway 14
Peru 14
Philippines 15
Poland 9
Portugal 9
Republic of Cyprus 9
Republic of Korea 15
Romania 9
Russian Federation 16
Singapore 16
Slovakia 9
Slovenia 9
South Africa 17
Spain 9
Sweden 9
Switzerland 17
Taiwan 18
Thailand 18
Turkey 19
United Arab Emirates 19
United Kingdom 9
United States 20
Uruguay 20

EU member states after July 1, 2016 9
EU member states before July 1, 2016 21
Introduction

Electronic and digital signatures represent a tremendous opportunity for organizations to get documents signed and close deals faster. When rolling out e-signatures globally, you need to be aware of the variety of electronic signature laws across the globe. This guide gives you a great place to start.

The guide covers the electronic signature laws of 47 countries, including all the largest economies. It gives a snapshot of each country’s electronic signature laws in the form of brief summaries. These provide a reference point for determining the scope of an organization’s use of electronic signatures in different jurisdictions. It is not meant to be an exhaustive or detailed legal analysis, but gives a solid place to start.

Each summary provides:

- The name of the electronic signature law and, where possible, a link to the best available online version of it. Be mindful that the links are sometimes to unofficial translations or other secondary materials. Nonetheless, they provide an excellent starting point.

- A succinct answer as to whether simple electronic signatures are considered legal, admissible and enforceable in that jurisdiction.

- A description of the type of electronic signature law that applies in that jurisdiction. Most laws fall into one of three categories: minimalist, two-tier or prescriptive.

- Types of transactions or other legal subject matter that are exempted from the law’s application or any other noteworthy issues in that jurisdiction.

Note: This information is intended to help you understand the legal framework of electronic signatures. However, Adobe cannot provide legal advice. The law of electronic signatures is constantly evolving. This guide is not intended as legal advice and should not serve as a substitute for professional legal advice. You should consult an attorney regarding your specific legal questions.

If you wish to conduct further research, the following resources may be helpful:

- *The Standards and Procedures for Electronic Records and Signatures (SPeRS)*
- *Electronic Signature & Records Association (ESRA)*
- *Database of Electronic Signature Legislation*
Definition of terms

Types of electronic signatures

Electronic signature: An electronic symbol or process attached to an agreement and executed or accepted by a person with the intent to sign the agreement or record. Examples include clicking an Accept button online, signing on a touch pad to approve a credit card purchase or typing one’s name on a signature line.

Digital signature: An electronic signature that uses an encrypted digital certificate to authenticate the identity of the signer. Digital signatures are sometimes referred to as advanced electronic signatures, qualified electronic signatures or other terms in jurisdictions outside the United States.

Types of electronic signature law

Permissive or minimalist: Simple electronic signatures have the same status as handwritten signatures as long as both parties agree to the use of electronic signatures.

Two-tier: Digital signatures have the same status as handwritten signatures, but electronic signatures are also legal and enforceable. These countries usually base their laws on the UNICTRAL Model Law on Electronic Signatures.

Prescriptive: The use of electronic and digital signatures is governed by restrictive, country-specific laws. Frequently there is no language addressing the enforceability of simple electronic signatures, but some allow parties to specify the acceptable form of signature in an agreement.

Recommended practices for electronic agreements

Consent: Agreements contain a provision stating that all parties agree that signing may be done electronically. Adobe Document Cloud eSign services include this provision automatically.

Opt-out option: Any parties to the document that desire to sign it using a handwritten signature must be given the option to do so.

Retention: All electronically signed agreements are retained in accordance with the organization’s usual document retention policies.

Audit trail: A copy of the signature audit trail, showing the time and identity of all signers, is attached to the executed agreement. This is done automatically with Adobe Document Cloud eSign services.

Circulation: An unaltered, fully executed, complete electronic copy of the document is sent to all parties for their reference and archiving. This is done automatically with Adobe Document Cloud eSign services.
Country summaries of electronic signature law

Argentina

**Electronic signature law**

*Digital Signature Law 25,506* (no translation available)

**Are electronic signatures legal, admissible and enforceable?**

Yes, electronic signatures are valid with prior consent from each party.

**Summary of law**

Argentina follows the UNCITRAL model law and is similar to the laws of many European Union member states. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Argentina's laws are somewhat different in that they primarily discuss the enforceability of digital or advanced electronic signatures. However, Section 1197 of the Argentine Civil Code provides that when the parties agree that they will accept electronic signatures as valid and that they won't challenge their validity, the agreement will bind both parties.

**Key restrictions**

Article 4 provides that the law does not apply to documents regarding death, family law or other highly personal matters.

Australia

**Electronic signature law**

*Electronic Transactions Act 1999*

**Are electronic signatures legal, admissible and enforceable?**

Yes, Part 10 states that one can meet the legal requirement for a handwritten signature by using an electronic signature or communication.

**Summary of law**

Australia's electronic signature law is considered a permissive or minimalist law. This means that it allows nearly all documents to be signed using simple electronic signatures. It is very similar to the U.S. law, with minimal requirements and clear enforceability. One only needs to have a means to reasonably identify the person signing and show evidence of their agreement. Of course, one should always get the consent of the signing party to do business electronically and follow standard record retention processes.

**Key restrictions**

The law does not apply to documents related to migration and citizenship. In addition, some regions have laws that provide that the law does not apply to wills, powers of attorney and some real estate transactions. However, there is no exception to the law that applies to standard business agreements.
**Bermuda**

**Electronic signature law**
*Electronic Transactions Act 1999*

Are electronic signatures legal, admissible and enforceable?
Yes, Section 11 of the Electronic Transactions Act recognizes electronic signatures as legal and enforceable, while Section 14 provides for their admissibility.

Summary of law
Bermuda’s law provides for the enforcement of both simple electronic signatures and digital signatures (sometimes called certified electronic signatures). It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case. Electronic signatures are presumed valid unless proof to the contrary is produced.

Key restrictions
Some real estate agreements and wills are exempted from the law.

---

**Brazil**

**Electronic signature law**
*Provisional Measure 2200-2, August 24th 2001 (unofficial translation)*

Are electronic signatures legal, admissible and enforceable?
Brazil’s law allows only for electronic signatures that utilize the Brazilian public key infrastructure (PKI). While these government-authorized signatures are legal, the use of simple electronic signatures is not provided for under the law.

Summary of law
Brazil generally follows the UNCITRAL Model Law on Electronic Signatures. However, under Article 1, it imposes the additional restriction of allowing only its own version of PKI to be legally recognized. Documents and signatures that use this PKI are considered legal and enforceable for all public and private purposes under Article 10.

Key restrictions
There are no critical restrictions under the law.
Canada

Electronic signature law
*Personal Information Protection and Electronic Documents Act, SC 2000, cS*

Are electronic signatures legal, admissible and enforceable?
Yes, the laws of Canada and each of its provinces explicitly grant electronic signatures the same status as handwritten signatures.

Summary of law
Canada’s laws follow the permissive approach. These minimalistic, or permissive, laws permit the use of electronic signatures for virtually all types of agreements. However, it is important to obtain the prior consent of all parties to conduct business electronically. Electronic signatures are presumed valid unless proof to the contrary is produced.

Key restrictions
Some real estate agreements, wills, estate agreements and powers of attorney are excluded from the law. There is some variation among the provinces respecting restrictions. See, for example, Quebec’s *Act to Establish a Legal Framework for Information Technology.*

Chile

Electronic signature law
*Law 19.799* and *Decree 181* (no translations available)

Are electronic signatures legal, admissible and enforceable?
Yes, Article 3 of Law 19.799 recognizes electronic signatures as legal and enforceable, while Article 5 provides for their admissibility.

Summary of law
Chile’s laws provide for the enforcement of both simple electronic signatures and digital signatures (called advanced or certified signatures). It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case. Electronic signatures are presumed valid unless proof to the contrary is produced.

Key restrictions
Agreements and documents related to acts or contracts where the law requires the personal attendance of one or more of the parties and those related to family law are exempted from the law.
China

Electronic signature law
Electronic Signature Law of the People's Republic of China

Are electronic signatures legal, admissible and enforceable?
Yes, Article 14 recognizes electronic signatures as legal and enforceable, while Articles 7 and 8 provide for their admissibility.

Summary of law
China's law is modeled on a combination of the EU Directive on Electronic Signatures, UNCITRAL Model Laws and United Nations Conventions on Electronic Communications in International Contracts. It provides for the enforcement of both simple electronic signatures and digital signatures. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case. Electronic signatures are presumed valid unless proof to the contrary is produced.

Despite the clear legal support for electronic signatures, some judges in China are still averse to recognizing them. As a result, you may wish to use handwritten signatures for more sensitive matters like employment contracts.

Key restrictions
Agreements related to personal relationships (such as marriage, adoption, inheritance), some real estate agreements and agreements related to the suspension of public utilities are exempted from the law.

Colombia

Electronic signature law
Several laws in Colombia address electronic signatures, including Law 527 of 1999, Law 1150 of 2007 (Public Procurement), Law 962 of 2005 (Electronic Invoice) and Law 964 of 2005 (Electronic Securities) (no links available)

Are electronic signatures legal, admissible and enforceable?
Yes, the law provides that the parties may use electronic signatures with consent.

Summary of law
Electronic signatures are used in both the public and private sectors in Colombia. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Legal rulings regarding electronic signatures have been somewhat general and do not address specific types of electronic signature. However, a Colombian Supreme Court decision in December 16, 2010, included digital and electronic signatures as recognized legal categories under Law 527. Obtaining consent prior to using electronic signatures is a good practice to ensure enforceability.

Key restrictions
Conveyance of real estate rights, aircraft, ships, corporations or other business associations; bylaws; mortgage agreements; unlimited agency agreements and incorporation of branches are exempted from the law.
EU member states after July 1, 2016

Electronic signature law

Effective July 1, 2016 — *Electronic Identification and Authentication Services Regulation (910/2014/EC)*

Current law, valid until July 1, 2016 — See country-by-country listings.

Are electronic signatures legal, admissible and enforceable?

Yes, electronic signatures are valid with prior consent.

Summary of law

In 1999, the European Union passed the Electronic Signature Directive (1999/93/EC) which member states used as the foundation for country-specific laws. On July 23, 2014, the EU adopted its replacement, the Electronic Identification and Trust Services Regulation (910/2014/EC). Commonly referred to as eIDAS, the regulation establishes a new legal structure for electronic identification, signatures, seals and documents throughout the EU. eIDAS will come into effect on July 1, 2016. On that date, the existing EU directive as well any laws of EU member states that are inconsistent with eIDAS will be automatically repealed, replaced or modified. For the first time, there will be a consistent legal framework and a single market for the recognition of electronic signatures and identities across all of the EU. This provides companies with a predictable legal environment in which to develop and expand the use of electronic signatures in the EU.

Article 25 of the eIDAS maintains the fundamental legal rule that all electronic signatures and verification services shall be admissible as evidence in legal proceedings. This includes electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.

**eIDAS and basic electronic signatures**

The basic definition of electronic signature is unchanged under eIDAS with respect to the earlier regulation. The law holds that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely based on the fact that it is in electronic form.

**eIDAS and advanced electronic signatures**

The regulation introduces a new definition for advanced electronic signatures. Advanced electronic signatures allow unique identification and authentication of the signer of a document enable the verification of the integrity of the signed agreement, typically through the issuance of a digital certificate by a certificate authority to that signer.

**eIDAS and qualified electronic signatures**

Another new definition under eIDAS is the qualified electronic signatures. While both advanced and qualified electronic signatures are uniquely linked to the signer, qualified electronic signatures are based on qualified certificates. Qualified certificates can be issued only by a certificate authority that has been accredited and supervised by authorities designated by the EU member states and must meet the requirements of eIDAS. Qualified certificates must also be stored on a qualified signature creation device such as a smart card, a USB token or a cloud-based hardware security module (HSM). While both basic electronic signatures and advanced electronic signatures are legal, admissible and enforceable under eIDAS, only qualified electronic signatures are deemed to be legally identical to handwritten signatures. Importantly, they are also the only type of electronic signature that will be mutual recognized by all of the EU member states. Thus, while it is not necessary to use a qualified electronic signature in every instance, it is a useful tool when executing some types of agreements.
Hong Kong

**Electronic signature law**

*Electronic Transactions Ordinance*

Are electronic signatures legal, admissible and enforceable?

Yes, Section 6(1) states that an electronic signature may be used to satisfy the legal requirement for a handwritten signature. Section 17(2) states that electronic records may be used in place of paper records and that those records will have the same legal enforceability as paper records.

**Summary of law**

Hong Kong follows the European Union and the UNCITRAL model law in that its laws provide for the enforcement of both simple electronic signatures and digital signatures (sometimes called advanced electronic signatures). It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

One must get consent to do business electronically, but that consent doesn’t need to be explicit. It can be inferred from behavior such as receiving and signing documents electronically.

**Key restrictions**

The law excludes wills, powers of attorney, government leases and some real estate transactions.

India

**Electronic signature law**

*The Information Technology Act, 2000*, further amended in 2006 and 2008

Are electronic signatures legal, admissible and enforceable?

Yes, with consent.

**Summary of law**

India’s laws provide for the enforcement of both simple electronic signatures and digital signatures (sometimes called advanced electronic signatures). It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Electronic signatures are presumed valid unless proof to the contrary is produced. Specifically, section 10A provides that where an agreement is "expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose." Further, if one obtains consent to use electronic signatures, the courts will be even more likely to uphold their use.

When using digital signatures in India, there are additional technical and legal requirements. Section 1535 in particular specifies standards for entities that issue digital certificates.

**Key restrictions**

Agreements related to powers of attorney, wills and real estate are exempted from the law. In addition, the requirement that many transactions must use stamped paper hinders adoption.
Electronic signature law

Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions

Are electronic signatures legal, admissible and enforceable?
Yes, but only those digital signatures that have been created using a digital certificate provider that has been registered with the Ministry of Communication and Information Technology and that has servers located in Indonesia are enforceable.

Summary of law
All forms of electronic signatures must meet the requirements under Law Number 11 of 2008, which includes the registration and certification of public electronic systems, registration of software for services and electronic agents and certification of all hardware, as well as the requirement that all data centers and disaster recovery centers be located in Indonesia. Any digital certificates must be issued by a certification provider approved by government agencies.

Key restrictions
Notarial deeds, letters of court summons and bond certificates are excluded from the law.

Electronic signature law

Electronic Signature Law, 5761 - 2001

Are electronic signatures legal, admissible and enforceable?
Chapter 2 requires the use of a certified electronic signature (sometimes called advanced electronic signatures) to satisfy laws requiring a signature on a document.

Summary of law
Israel's Electronic Signature Law is modeled on the EU Directive on Electronic Signatures, but it does not permit the use of electronic signatures when a signature is required on a document. Instead, Israel requires the use of a digital signature. However, some documents may not require a signature to be enforceable. In these situations, an electronic signature solution may be appropriate to track and manage the final, approved version of a document.

Key restrictions
Israel's Electronic Signature Law does not contain any restrictions on the type of agreement it applies to when using a digital signature.
Japan

Electronic signature law

*Law Concerning Electronic Signatures and Certification Services* (unofficial translation)

**Are electronic signatures legal, admissible and enforceable?**
Yes, Japanese law allows electronic signatures for most types of agreements.

**Summary of law**

In Japan, a signature cannot be denied enforceability simply because it is in electronic form. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

While the use of a red seal stamp is common for signatures, electronic signatures are supported by the *Law Concerning Electronic Signatures and Certification Services*. Also, Japanese evidence rules generally permit the parties to an agreement to agree on the form of acceptance of that agreement.

**Key restrictions**

It is advisable to avoid using electronic signatures for documents related to real property transfers and wills.

Malaysia

Electronic signature law

*Digital Signature Act*

**Are electronic signatures legal, admissible and enforceable?**

Section 62 requires the use of a digital signature (sometimes called advanced electronic signatures) where the law requires a signature.

**Summary of law**

Malaysia’s Digital Signature Act is modeled on the UNCITRAL Model Law on Electronic Signatures but does not permit the use of electronic signatures when a signature is required on a document. Instead, Malaysia requires the use of a digital signature. However, some documents may not require a signature to be enforceable. In these situations, an electronic signature solution may be appropriate to track and manage the final, approved version of a document.

**Key restrictions**

Malaysia’s electronic signature law does not contain any restrictions on the type of agreement it applies to when using a digital signature.
Mexico

Electronic signature law
Several laws (no links available)

Are electronic signatures legal, admissible and enforceable?
Mexico's laws generally permit parties to state their consent though electronic means.

Summary of law
Mexico is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Mexico amended several laws, including the Code of Commerce, Federal Civil Code and Federal Code on Civil Procedures, to permit the use of electronic signatures and advanced electronic signatures. Under this system, advanced electronic signatures are preferred, but parties are generally free to determine the form of acceptance for an agreement.

Key restrictions
Digital signatures may be required for the certification of official documents and for documents related to tax obligations.

New Zealand

Electronic signature law
Electronic Transactions Act

Are electronic signatures legal, admissible and enforceable?
Yes, Section 8 provides that information will not be denied legal effect solely because it is in electronic form.

Summary of law
New Zealand's electronic signature law can be classified as permissive or minimalist. Under the law, parties to an agreement can freely agree on the type of signature to use, including simple electronic signatures. The primary requirements are that the parties agree on the form of signature, and the electronic document remains readily accessible to the parties.

Key restrictions
While the law does not exclude particular types of agreements, some agreements, like real estate transfers and wills, have additional requirements.
Norway

Electronic signature law
*Electronic Signatures Act 2001 (no translation available)*

**Are electronic signatures legal, admissible and enforceable?**
Yes, Section 6 recognizes electronic signatures as legal and enforceable.

**Summary of law**
Norway follows the European Union model. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Electronic signatures are presumed valid unless proof to the contrary is produced, but they do not have the same status as digital (or qualified electronic) signatures.

**Key restrictions**
Debt certificates, premarital agreements and a board’s signing of annual accounts are examples of excluded transactions.

Peru

Electronic signature law
Digital Certificates and Signatures Law, Law No. 27269 (no translation available)

**Are electronic signatures legal, admissible and enforceable?**
Peru recognizes only the legal status of digital or advanced electronic signatures.

**Summary of law**
In Peru, all forms of electronic signature must include a digital certificate. Peruvian law specifies the minimum requirements for digital certificates and for the issuers of digital certificates. To be considered valid, a digital certificate must be issued by a certification provider that meets these standards. Peru recognizes the validity of digital certificates issued in other countries only if they meet Peruvian standards.

**Key restrictions**
There are no critical exceptions to the law.
**Philippines**

**Electronic signature law**

*Republic Act No. 8792: An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents*

**Are electronic signatures legal, admissible and enforceable?**

Section 8 specifies that all signatures must use a digital certificate.

**Summary of law**

The Philippines provides for the enforceability of digital signatures. While parties are free to agree between themselves that electronic signatures will be binding, that agreement could increase the enforceability risk. For all practical purposes, digital signatures should be used.

**Key restrictions**

No restrictions are noted.

---

**Republic of Korea**

**Electronic signature law**

*Digital Signature Act*

**Are electronic signatures legal, admissible and enforceable?**

Yes, as long as the parties explicitly consent to electronic signatures per Article 3(3) of the enactment.

**Summary of law**

The Republic of Korea’s e-signature laws are modeled after a combination of the EU Directive on Electronic Signatures and UNCITRAL Model Law. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Like many other countries, consent is required for allowing electronic signatures. However, if no such explicit agreement exists between the parties or the identity of the signer or the authenticity or integrity of the message sent is questioned, the effect of the electronic signature has to be determined by interpreting the true intention of the parties in accordance with the general principle of contract interpretation.

**Key restrictions**

There are no critical restrictions.
**Russian Federation**

**Electronic signature law**
Federal Law No. 63-FZ, “On Digital Signature” (July 01, 2011)
Part Four of Civil Code of the Russian Federation (Art. 160) (no links available)

**Are electronic signatures legal, admissible and enforceable?**
Yes, Russian law recognizes electronic signatures as legal, admissible and enforceable when the parties explicitly agree to use them. However, for enforceable digital signatures, Russia requires that one use a certificate and service provider that has been certified by the Russian government.

**Summary of law**
Russian courts have held that a signature may not be denied validity simply because it is electronic. However, to be clearly enforceable, digital signatures must be exchanged through a government-certified, specialized service provider that acts as an electronic courier in order to enable electronic document exchange.

**Key restrictions**
There are no critical exceptions to the law.

---

**Singapore**

**Electronic signature law**
*Electronic Transactions Act 2010*

**Are electronic signatures legal, admissible and enforceable?**
Yes, Section 8 states that one can meet the legal requirement for a handwritten signature by using an electronic signature or communication.

**Summary of law**
Singapore is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Under the law, the signature method used must be either “(i) as reliable as appropriate for the purpose for which the electronic record was generated or communicated, or (ii) proven in fact to have identified the signatory and to indicate signatory’s intention with respect to the information by itself or together with further evidence.”

**Key restrictions**
The law excludes wills, negotiable instruments, powers of attorney and some real estate transactions.
South Africa

Electronic signature law
*Electronic Communications and Transactions Act, 2002 (Act No. 25)*

Are electronic signatures legal, admissible and enforceable?
Yes, as long as the parties consent to electronic signatures per Section 13.

Summary of law
South Africa generally follows the EU Directive on Electronic Signatures. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Consent is the prerequisite for allowing electronic signatures. However, according to Section 13(5) of the Electronic Communications and Transactions Act, if the parties have not agreed on a specific type of electronic signature, as long as there is a) a method to identify the person and to indicate the person’s approval of the information communicated; and b) the method is reliable and appropriate for the purpose for which the information was communicated, electronic signatures are also legal, admissible and enforceable in South Africa.

Key restrictions
The law excludes long-term leases; transfers of property; the execution, retention and presentation of wills; and bills of exchange.

Switzerland

Electronic signature law
*Federal Law on Electronic Signatures (no translation available)*

Are electronic signatures legal, admissible and enforceable?
Yes, Article 14 states that electronic signatures may replace handwritten signatures.

Summary of law
Switzerland follows the UNICTRAL model law and is similar to the laws of many European Union member states. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Key restrictions
There are no noteworthy exceptions to the law, but some caution may be warranted in the areas of real estate, notarized documents and wills and trusts.
Taiwan

Electronic signature law
Electronic Signatures Act 2001-11-14

Are electronic signatures legal, admissible and enforceable?
Yes, Article 9 states that electronic signatures may replace handwritten signatures. Article 4 provides that if a law or regulation requires information be provided in writing, the requirement may be satisfied with an electronic record.

Summary of law
Taiwan follows the UNCITRAL model law and is similar to the laws of many European Union member states. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Key restrictions
Getting express consent to do business electronically is particularly important in Taiwan. Taiwanese law does not view a party's name on an email as an adequate electronic signature. A number of government agencies have issued bulletins excepting themselves from the law.

Thailand

Electronic signature law

Are electronic signatures legal, admissible and enforceable?
Yes, Section 9 states that electronic signatures may replace handwritten signatures. Sections 7 and 8 provide that if a law or regulation requires information to be provided in writing, the requirement may be satisfied with an electronic record.

Summary of law
ETA Section 13 provides that an offer or acceptance in entering into an agreement may be expressed by means of a data message. An agreement shall not be denied legal effect solely on the ground that such offer or acceptance is made in the form of a data message. Electronic signatures are presumed valid unless proof to the contrary is produced.

Key restrictions
There are no critical exceptions to the law.
Turkey

Electronic signature law
Electronic Signature Law (Elektronik Imza Kanunu) No:5070 (no link available)

Are electronic signatures legal, admissible and enforceable?
Turkey follows the UNCITRAL model law and is similar to the laws of many European Union member states. However, its laws are focused solely on the legality of what are called digital, advanced or qualified electronic signatures. These types of signatures require that the signing party have a digital certificate that has been issued by a qualified service provider. Those advanced electronic signatures have the same legal effect as handwritten signatures. There is no clear provision for simple electronic signatures under Turkish law.

Summary of law
Articles 5 and 22 provide that advanced electronic signatures have the same status as handwritten signatures. The burden is on the party challenging such signatures to prove they are invalid. An agreement shall not be denied legal effect solely on the grounds that such offer or acceptance is made electronically.

Key restrictions
There are no critical exceptions to the law.

United Arab Emirates

Electronic signature law
Electronic Transactions and Commerce Law No. 2 of 2002

Are electronic signatures legal, admissible and enforceable?
Yes, the UAE follows the UNCITRAL model law and is similar to the laws of many European Union member states. Electronic signatures have the same status as handwritten signatures. Consent to do business electronically can be inferred from circumstances and does not need to be explicit.

Summary of law
Article 10(1) states that legal signature requirements may be met with the use of an electronic signature. Article 7(1) states that an electronic communication shall not be denied legal effect or enforceability solely on the ground that it is in electronic form.

Key restrictions
One must obtain the explicit consent of the government when seeking to transact electronically. Transactions relating to marriage, divorce, wills, real estate and negotiable instruments are exempted from the law.
United States

**Electronic signature law:**
*Electronic Signatures in Global and National Commerce Act* (ESIGN) and *Uniform Electronic Transactions Act* (UETA)

**Are electronic signatures legal, admissible and enforceable?**
Yes, both the ESIGN Act and UETA provide that a signature will not be denied legal effect or enforceability solely because it is in electronic form.

**Summary of law**
The federal government adopted ESIGN in 2000. In addition, every state has adopted an electronic signature law, with 47 adopting a version based on UETA. These minimalist, or permissive, laws permit the use of electronic signatures for virtually all types of agreements. However, it is important to obtain the prior consent of all parties to conduct business electronically.

**Key restrictions**
The ESIGN Act and most state laws exclude real property transfers, wills and some legally required notices to consumers.

---

Uruguay

**Electronic signature law**
Law No. 18.600 on Electronic Documents and Electronic Signatures (no link available)

**Are electronic signatures legal, admissible and enforceable?**
Yes, the law allows the parties to agree privately to the form of signature.

**Summary of law**
The law is somewhat unusual in that it allows the parties to challenge consent after it has been given. That is, the parties may agree to transact business electronically and sign the document electronically, but this will not stop either party from challenging that consent at a later date. On the other hand, there is evidence that electronic signatures are used commonly in Uruguay and are submitted in court filings.

**Key restrictions**
One should be cautious of transactions that must be notarized or that relate to real estate.
EU member states before July 1, 2016

In 1999, the European Union passed the Electronic Signature Directive (1999/93/EC) which member states used as the foundation for the country-specific laws described in this section. On July 1, 2016 the European Union Electronic Identification and Trust Services Regulation (eIDAS) will take effect—creating a single, standardized regulation for all 28 member states. On that date, the existing EU Directive as well any laws of EU member states that are inconsistent with eIDAS will be automatically repealed, replaced or modified.

Current laws:

<table>
<thead>
<tr>
<th>Country</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>24</td>
</tr>
<tr>
<td>Belgium</td>
<td>24</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>25</td>
</tr>
<tr>
<td>Denmark</td>
<td>25</td>
</tr>
<tr>
<td>Finland</td>
<td>26</td>
</tr>
<tr>
<td>France</td>
<td>26</td>
</tr>
<tr>
<td>Germany</td>
<td>27</td>
</tr>
<tr>
<td>Hungary</td>
<td>27</td>
</tr>
<tr>
<td>Ireland</td>
<td>28</td>
</tr>
<tr>
<td>Italy</td>
<td>28</td>
</tr>
<tr>
<td>Netherlands</td>
<td>29</td>
</tr>
<tr>
<td>Poland</td>
<td>29</td>
</tr>
<tr>
<td>Portugal</td>
<td>30</td>
</tr>
<tr>
<td>Romania</td>
<td>30</td>
</tr>
<tr>
<td>Spain</td>
<td>31</td>
</tr>
<tr>
<td>Sweden</td>
<td>31</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>32</td>
</tr>
</tbody>
</table>
Austria

Current electronic signature law valid through June 2016. (Starting July 1, 2016, the new elDAS regulation will apply.)

Federal Electronic Signature Law

Are electronic signatures legal, admissible and enforceable?
Austria’s law focuses on the enforceability of digital signatures. However, Section 3(1) provides that signatures may not be excluded merely because they are in electronic form.

Summary of law
Austria follows the UNCITRAL model law and is similar to the laws of many European Union member states. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

However, Austria’s laws are somewhat different in that they primarily provide for the enforceability of digital or advanced electronic signatures. However, electronic signatures are nonetheless enforceable, although it is especially important to obtain consent from the other party prior to using them.

Key restrictions
The law does not apply to legal transactions under family and inheritance law, documents that must be notarized or real estate transactions where a notarial deed must be entered in the land register, companies register or other official register.

Belgium

Current electronic signature law valid through June 2016. (Starting July 1, 2016, the new elDAS regulation will apply.)

9 July 2001—Law determining some rules concerning the legal framework of electronic signatures and certification services (unofficial translation)

Are electronic signatures legal, admissible and enforceable?
Yes, Civil Code Section 1322 recognizes electronic signatures as legal and enforceable.

Summary of law
Belgium follows the UNCITRAL model law and is similar to the laws of many European Union member states. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Electronic signatures are presumed valid unless proof to the contrary is produced. Article 4, Section 5, provides that no electronic signature will be denied simply because it is in electronic form or is not based on a digital certificate.

Key restrictions
There are no critical exceptions to the law.
Czech Republic

Current electronic signature law valid through June 2016. (Starting July 1, 2016, the new eIDAS regulation will apply.)

227/2000 Coll. ACT of 29 June 2000 on electronic signatures and on the amendment to certain acts (Electronic Signatures Act) as subsequently amended

Are electronic signatures legal, admissible and enforceable?
Yes, Section 3 specifies that a document is considered signed if it is signed with an electronic signature. Parties may still request handwritten signatures.

Summary of law
The Czech Republic follows the UNCITRAL model law and is similar to the laws of many European Union member states. It is considered a two-tier Jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Electronic signatures are presumed valid unless proof to the contrary is produced. Section 3 of the 227/2000 Coll. ACT states, "A data message shall be signed if it is furnished with an electronic signature."

Key restrictions
Real estate purchases or leases are exempted from the law.

Denmark

Current electronic signature law valid through June 2016. (Starting July 1, 2016, the new eIDAS regulation will apply.)

Bill on Electronic Signatures

Are electronic signatures legal, admissible and enforceable?
Denmark’s law allows only for the enforceability of digital signatures. While digital or advanced electronic signatures are legal, the use of simple electronic signatures is not provided for under the law.

Summary of law
Denmark follows the model law that many European Union member states do. However, it is unusual in that it does not have a provision recognizing simple electronic signatures.

The law also provides rules for the certification authorities that issue digital certificates. It is limited to certification authorities established in Denmark and does not specify any special requirements concerning certification authorities and electronic signatures originating in other countries. However, it does make it possible for certificates issued by them to be recognized in the same way as certificates issued by Danish certification authorities.

Key restrictions
There are no critical restrictions.
Finland

Current electronic signature law valid through June 2016.
(Starting July 1, 2016, the new eIDAS regulation will apply.)

Act on Strong Electronic Identification and Electronic Signatures (617/2009)

Are electronic signatures legal, admissible and enforceable?
Yes, with consent.

Summary of law
Finland follows the UNCITRAL model law and is similar to the laws of many European Union member states. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Electronic signatures are presumed valid unless proof to the contrary is produced.

Key restrictions
Agreements related to the purchase or transfer of real estate and family law or inheritance are exempted from the law.

France

Current electronic signature law valid through June 2016.
(Starting July 1, 2016, the new eIDAS regulation will apply.)

Law No. 2000-230 of 13 March 2000 Adapting the Right of Proof to Information Technologies and Electronic Signatures (French), which modifies Civil Code Article 1316 (English) and other laws related to signatures and records

Are electronic signatures legal, admissible and enforceable?
Yes, Civil Code Section 1316-4 recognizes electronic signatures as legal and enforceable, while Section 1316-1 provides for their admissibility.

Summary of law
France follows the UNCITRAL model law and is similar to the laws of many European Union member states. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Electronic signatures are presumed valid unless proof to the contrary is produced.

Key restrictions
Agreements related to marriage, documents that must be notarized, some real estate agreements and labor agreements are exempted from the law.
Germany

Current electronic signature law valid through June 2016. (Starting July 1, 2016, the new eIDAS regulation will apply.)

Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations

Are electronic signatures legal, admissible and enforceable?

Yes.

Summary of law

Germany follows the UNCITRAL model law and is similar to the laws of many European Union member states. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

In Germany, 95% of all agreements are signed only for the purpose of demonstrability of the agreement, and not for legal reasons. Therefore, all of these agreements require only a simple electronic signature.

Key restrictions

Some agreements require a qualified digital signature. In addition, agreements related to real estate, notarized documents and marriage are exempted from the law.

Hungary

Current electronic signature law valid through June 2016. (Starting July 1, 2016, the new eIDAS regulation will apply.)

ACT XXXV of 2001

Are electronic signatures legal, admissible and enforceable?

Yes, if legislation does not specifically require a handwritten signature for a document and both parties consent to electronic signature, then electronic signatures are enforced.

Summary of law

Hungary’s law regarding electronic signature is based on the EU Directive on Electronic Signatures. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Section 3(1) of Act XXXV of 2001 states: “(1) Acceptance of an electronic signature, or document, including if used as evidence, cannot be denied and their suitability for legal statement and their legal force cannot be disputed...solely on the grounds that the signature, or the document exists only in electronic format."

Key restrictions

Section 3(2) of Act XXXV of 2001 states: “In connection with the legal relationships referred to in Sections 598-684 of the Civil Code of the Republic of Hungary and in Act IV of 1952 on Marriage, family and Legal Custody, the relevant documents cannot be made with electronic signatures and in electronic format only, by abolishing the use of any format other than electronic.”
Ireland

Current electronic signature law valid through June 2016.
(Starting July 1, 2016, the new eIDAS regulation will apply.)

*Electronic Commerce Act, 2000*

Are electronic signatures legal, admissible and enforceable?
Yes, Section 12(b) provides that an electronic signature may be used anywhere that a handwritten signature is required.

Summary of law
Ireland follows the UNCITRAL model law and is similar to the laws of many European Union member states. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Electronic signatures are presumed valid unless proof to the contrary is produced.

Key restrictions
The law does not apply to wills, trusts, powers of attorney or real property transactions.

Italy

Current electronic signature law valid through June 2016.
(Starting July 1, 2016, the new eIDAS regulation will apply.)

*March 7, 2005 Legislative Decree No. 82* (no translation available)

Are electronic signatures legal, admissible and enforceable?
Italy's electronic signature law favors the use of digital signatures (sometimes called advanced electronic signatures). However, courts are allowed to determine the evidentiary value of most evidence, including electronic signatures.

Summary of law
While Italy's electronic signature law is modeled on the EU Directive on Electronic Signatures, it does not explicitly permit the use of electronic signatures. However, some documents may not require a signature to be enforceable. In these situations, an electronic signature may be admissible to establish the final, approved version of a document.

Key restrictions
When using a qualified electronic signature, Italy's electronic signature law does not exclude any types of agreements.
Netherlands

**Current electronic signature law valid through June 2016.**
(Starting July 1, 2016, the new eIDAS regulation will apply.)

*Electronic Signatures Act*

**Are electronic signatures legal, admissible and enforceable?**

Yes, Article 3.15a provides that an electronic signature has the same legal effect as a handwritten signature provided certain conditions are met.

**Summary of law**

Following the EU Directive on Electronic Signatures, Dutch law encompasses both electronic and digital signatures. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

The law specifically states that an electronic signature cannot be considered unreliable solely because it is not based on a qualified certificate (a fundamental element of digital signatures). In practice, parties are generally permitted to agree on the method and form of agreement.

**Key restrictions**

The law does not explicitly exclude any types of agreements.

---

Poland

**Current electronic signature law valid through June 2016.**
(Starting July 1, 2016, the new eIDAS regulation will apply.)

*The Act of 18 Sept. 2001 on Electronic Signature*

**Are electronic signatures legal, admissible and enforceable?**

Yes. As long as the parties consent to an electronic signature, it is enforceable for all agreements where the law does not provide a special form.

**Summary of law**

Poland follows the EU Directive on Electronic Signatures. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Article 8 of Poland’s Electronic Signature law states: "The electronic signature may not be denied validity and legal effectiveness solely on the grounds that it is in the electronic form or that the signature verification data do not have a qualified certificate or that the signature has not been created with the use of a secure signature creation device."

**Key restrictions**

Agreements related to any transfers of real property, registered pledges or transfer of: a) shares in a limited liability company; b) business; and c) shares in a joint stock company, testaments, check and bill of exchange, confirmation of insurance and employment agreements are exempted from the law.
Portugal

Current electronic signature law valid through June 2016. (Starting July 1, 2016, the new eIDAS regulation will apply.)

Decree-Law no. 290-D/99, of 2 of August
Decree-Law no. 62/2003 of 3 April Published in the D.R. no. 79 (Series I-A), of 3 of April
Decree-Law no. 234/2000, of 25 of September
Decree-Law no. 256/2003, of 21 of October

Are electronic signatures legal, admissible and enforceable?
Yes, Article 3, Section 4, provides for electronic signatures as long as the parties explicitly consent to their use.

Summary of law
Portugal's e-signature laws follow the EU Directive on Electronic Signatures. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Though digital (or advanced) electronic signatures are favored, Article 3 provides that so long as the signature method of agreement is agreed upon between the parties, it will be deemed valid.

Key restrictions
There are no critical restrictions.

Romania

Current electronic signature law valid through June 2016. (Starting July 1, 2016, the new eIDAS regulation will apply.)

Law on the Electronic Signature 2001
Law on Electronic Commerce 2002

Are electronic signatures legal, admissible and enforceable?
Yes, electronic signatures may be used, even if the parties did not initially express a desire to use them. This consent may be communicated verbally or in writing.

Summary of law
Romania follows the European Union in that its laws provide for the enforcement of both simple electronic signatures and digital signatures (sometimes called advanced electronic signatures). It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Key restrictions
Real estate and labor agreements require a digital signature.
Spain

Current electronic signature law valid through June 2016. (Starting July 1, 2016, the new eIDAS regulation will apply.)

Ley 59/2003, de 19 de diciembre, de firma electrónica (no translation available)

Are electronic signatures legal, admissible and enforceable?
Yes in accordance with Articles 3 and 26.

Summary of law
Spain’s e-signature law is modeled after the EU Directive on Electronic Signatures. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

It is not necessary for the parties to agree on the use of electronic means for signing such agreements. As long as the recipient accepts the terms and conditions of the agreement by clicking the "I agree" button or sends an email, the agreement should be considered enforceable and such acceptance will be admissible as evidence in court. Note that public authorities may establish additional conditions to impose electronic dates on electronic documents as a means to verify the time that action has been made.

Key restrictions
There are no critical restrictions.

Sweden

Current electronic signature law valid through June 2016. (Starting July 1, 2016, the new eIDAS regulation will apply.)

Qualified Electronic Signatures Act (SFS 2000:832)

Are electronic signatures legal, admissible and enforceable?
Section 17 states that only qualified electronic signatures that use a digital certificate may be used in place of handwritten signatures.

Summary of law
Sweden follows the UNCITRAL model law and is similar to the laws of many European Union member states. However, its laws are focused solely on the legality of what are called digital, advanced or qualified electronic signatures. These types of signatures require that the signing party have a digital certificate that has been issued by a qualified service provider. There is no clear provision for simple electronic signatures under Swedish law.

Key restrictions
Some agreements with government entities may be exempted.
United Kingdom

Current electronic signature law valid through June 2016.
(Starting July 1, 2016, the new elDAS regulation will apply.)

Electronic Communications Act 2000

Are electronic signatures legal, admissible and enforceable?
Yes, the U.K. law is similar to the U.S. law because it allows nearly anything in electronic form that is logically associated with a document with the intent to indicate agreement to function as an electronic signature.

Summary of law
Section 7(2) defines an electronic signature as anything in electronic form incorporated into or otherwise logically associated with any electronic communication or data that purports to be incorporated for the purpose of establishing the authenticity or integrity of communications or data. The law also provides for digital or advanced electronic signatures, but there is no legal reason to utilize them.

Key restrictions
There are few exceptions to the law, but caution should be taken with transactions relating to marriage, divorce, wills, real estate and negotiable instruments.
Introduction

This summary provides a general overview of the legality of e-signatures and scanned contractual agreements, primarily in the context of commercial loan documentation. E-signatures refer to documents that are signed electronically, whereas scanned contractual agreements refer to documents that are printed, executed and then scanned. The legal arena within which these two matters reside is one that requires an understanding of both federal and provincial legislation, and as such, the sections that follow draw upon statutes from both levels of government. Please note that this summary should not be construed as offering legal advice, but rather, as providing important information that will be discussed during the panel discussion. Counsel should always be retained for all legal matters.

A. The Use of E-Signatures in the Canadian Legal Landscape

Subject to certain exceptions, namely whether there are any specific statutory formality requirements for signatures that apply to a type of document or signature, applicable Canadian federal and provincial law are generally permissive in relation to the use of e-signatures. This is the case so long as the e-signature technology used is reliable and meets the basic characteristics of an enforceable e-signature.

I. E-Signatures: A permissive legal landscape

A. General Regimes applicable to E-Signatures

1. Federal Bank Act

- Documents granting security under s. 427 of the Bank Act (Canada) (“BA”) may be signed electronically. Pursuant to s. 1002 BA, any requirement under the BA for an original wet ink signature could be satisfied by an e-signature, provided the prescribed security measures for such e-signature are maintained.

- However, internal requirements related to the Bank of Canada’s processes and practices provide that a notice of intention registered with the Bank of Canada still requires wet ink signature.

2. Provincial Statutory Requirements – Excluding Quebec

- All Canadian provinces and territories have adopted e-commerce legislation.

- Under the Electronic Commerce Act, 2000 (Ontario) (and the equivalent legislation in other common law provinces), unless the document is of a type that has statutorily prescribed form or signature requirements, an electronic signature will be valid and enforceable (to the same extent as a “wet signature”) as long as: (1) the electronic signature is reliable for the purpose of identifying the person; and (2) the association of the electronic signature with the relevant electronic document is reliable.

- Note that the provinces of Alberta and Prince Edward Island have unique regimes, especially so with the former.
3. Provincial Statutory Requirements – Quebec Only

- In general, Quebec’s Act to Establish a Legal Framework for Information Technology implements the principles of technological neutrality and functional equivalency (as between paper-based and electronic communications).

II. Exceptions

The generally permissive statutory framework in Canada is subject to exceptions. Whenever examining whether e-signatures are enforceable, one must assess whether there are any specific statutory formality requirements for signatures that apply to the type of document or signature. By way of example, we draw upon a non-exhaustive list of exceptions that apply in relation to the use of e-signatures with certain types of security documentation:

1. E-signature solutions cannot be used by financial institutions in Alberta with individuals as regards:
   a) an offer of financing with a guarantee embedded in the offer; or b) a stand-alone guarantee.

2. E-signatures cannot be used in Saskatchewan for guarantees which are related to farm land or other assets used in farming.

3. In Quebec, under the Consumer Protection Act contracts of credit, except demand loans (other than lines of credit), must be in paper form. However, this requirement does not apply in the case of “distance contracts”, which are contracts entered into without the merchant and the consumer being in one another’s presence. When the parties are not in each other’s presence, the contract does not have to be in paper form and can be signed electronically.

4. As alluded to above, we note that under current practices, documents granting security under s. 427 of the BA and registered with the Bank of Canada still require wet ink signature.

5. E-signature solutions should not be used in relation to immovable hypothecs and mortgages in the following provinces: British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, Nova Scotia, Newfoundland, New Brunswick and Prince Edward Island.

   Same should also not be used in Alberta or Nova Scotia in relation to any other documents of title or records that create or transfer interests in land (and in Nova Scotia, where such documents creating or transferring an interest in land require registration in order to be effective against third parties).

6. Finally, other than in New Brunswick, e-signature solutions should not be used with (a) wills and codicils; (b) trusts created by wills or codicils; (c) powers of attorney, to the extent that they are in respect of an individual’s financial affairs or personal care, (d) negotiable instruments, and (e) forms that involve the designation of a beneficiary since there is case law that suggests that a beneficiary designation amounts to a “testamentary disposition” and, like a will, may not be signed electronically.

---

1 Section 25 and 80 Consumer Protection Act (Quebec). For clarity, this means that contracts of credit for lines of credit must be in paper form pursuant to these provisions (unless they are “distance contracts”).

2 See Sections 25 and 54.1, Quebec CPA.
B. The Use of Scanned Agreements in the Canadian Legal Landscape

This section provides a brief overview on the generally permissive legal landscape related to the use of scanned agreements.

I. Scanned Documents: A permissive legal landscape

A. General Regimes Applicable to Scanned Documents

*Uniform Electronic Commerce Act (“UECA”)* – Most provinces have UECA-inspired legislation (except Manitoba). Even though Quebec’s regime is different in substance and form, practically, it is very similar.

- Central to the legislation based on the UECA is the principle that an electronic document will not be denied legal effect and enforceability simply because it is in electronic form.

- Other than certain specific categories of documents that are referenced in the applicable e-commerce legislation that must be retained in original paper form, documents may be converted into and retained in electronic form unless such conversion or retention of records or documents in electronic form is expressly prohibited or regulated by a statute applicable thereto.

*BA & the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (Canada)* – These two statutes regulate electronic records and documents, in certain respects.

- Generally, the relevant components of these statutes are aligned with the UECA-based provincial regimes.

*Uniform Electronic Evidence Act (“UEEA”)* – Most provinces in Canada, other than British Columbia and Newfoundland and Labrador, have adopted legislation based on the UEEA. Despite the different content and form under Quebec evidentiary rules, practically, the Quebec regime is very similar.

- Such legislation provides that electronic records will be admissible in court provided that the person wishing to have them admitted can prove that the record is authentic, is not hearsay and that it satisfies the “best evidence” rule.

- These tests for authenticity and hearsay are the same as would be required for paper records.

- UEEA-inspired provincial law provides that the best evidence rule in respect of an electronic record or document is satisfied on proof of the integrity of the electronic records system by or in which the electronic record or document was recorded and stored. Consequently, companies must demonstrate the integrity of their electronic records systems if they wish to have their electronic records or document be considered admissible in court.

- Once converted into electronic form, records must be retained in an appropriate manner in order to maintain their integrity. Most commentators agree that the guidelines approved by the CGSB in 2017, the Electronic Records as Documentary Evidence, CAN/CGSB 7234-2017, are the most appropriate and authoritative guidelines to follow when developing an electronic records system and the associated policies and procedures.
VANCOUVER
Suite 2400, 745 Thurlow Street
Vancouver BC  V6E 0C5
Tel: 604-643-7100  Fax: 604-643-7900

CALGARY
Suite 4000, 421 7th Avenue SW
Calgary AB  T2P 4K9
Tel: 403-260-3500  Fax: 403-260-3501

TORONTO
Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto ON  M5K 1E6
Tel: 416-362-1812  Fax: 416-868-0673

MONTRÉAL
Suite 2500
1000 De La Gauchetière Street West
Montréal QC  H3B 0A2
Tel: 514-397-4100  Fax: 514-875-6246

QUÉBEC CITY
500, Grande Allée Est, 9e étage
Québec QC  G1R 2J7
Tel: 418-521-3000  Fax: 418-521-3099

NEW YORK, US
55 West 46th Street Suite 2804
NEW YORK NY  10036
UNITED STATES
Tel: 646-940-8970  Fax: 646-940-8972

LONDON, UK
1 Angel Court, 18th Floor
London EC2R 7HJ
UNITED KINGDOM
Tel: +44 (0)20 7786 5700  Fax: +44 (0)20 7786 5702
Electronic Contracts and E-Signatures

Juliet M. Moringiello
Widener University Commonwealth Law School

Steve Weise
Proskauer Rose LLP

July 2019
Introduction

- Difference between e-signature and online agreements
- Relationship of UETA and E-SIGN
- Scope of UETA and E-SIGN
- Electronic signatures generally
- Formation of contracts online
- Terms of contracts formed online
- Post-formation terms and amendments
- ‘Smart’ Contracts
Difference between e-signature and online agreements

• E-signature is manner of ‘signing’ an agreement
• An e-signature can apply to a paper agreement or an agreement formed online
• An online agreement raises the question of when the agreement has been formed online, even if there is an agreement
Relationship between UETA and E-SIGN

- E-SIGN defers to state law if the state has adopted the substance of the official version of UETA or has adopted comparable “alternative procedures or requirements” for the use or acceptance of E-Records and E-Signatures, provided that they satisfy certain conditions including that they are “consistent with” Titles I and II of E-SIGN.
- 47 states plus DC and the USVI have adopted UETA, with revisions that are generally consistent with the official version of E-SIGN.
- New York did not adopt UETA and instead created and adopted the Electronic Signatures and Records Act (ESRA). Illinois, Washington and Puerto Rico also have unique E-Record/E-Signature statutes.
- Each of these unique state statutes validates E-Records and E-Signatures in a manner that is similar to E-SIGN and UETA. However, it is not clear that these statutes are similar enough to UETA to qualify for E-SIGN’s deferral to state law.
- Even if the state statutes are not similar enough to UETA to qualify for E-SIGN’s deferral, the ultimate result is generally the same.
- Because E-SIGN will apply if a state has not adopted UETA (or its equivalent), at least one of those laws will always apply.
Electronic Records Signatures

Generally — effect of e-signature

• The Uniform Electronic Transactions Act (UETA) and the federal Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 USC §§ 7001 et seq., are enabling statutes that place electronic records and signatures on a legal par with their paper and ink counterparts.

• They provide that records and signatures “may not be denied legal effect, validity or enforceability solely because [they] are in electronic form.”
Technology requirements?

• Each statute is technology-neutral.
• Unlike earlier “digital signature” laws, these statutes do not require the use of technologies to help verify either the identity of the signing party or the integrity of the record (document) itself. Similarly, they do not accord any preferred status to E-Records or E-Signatures created using technologies that do so.
Application to a ‘transaction’

• Subject to certain exclusions (such as wills and most of the UCC), UETA applies to E-Records and E-Signatures “relating to transactions,” with

• “transactions” defined to include any action “between two or more persons relating to the conduct of business, commercial or governmental affairs.”

• Subject to substantially the same exclusions as UETA, E-SIGN covers ‘any transaction in or affecting interstate or foreign commerce,’ with

• E-SIGN defines ‘transaction’ to include any action ‘relating to the conduct of business, consumer or commercial affairs between two or more persons.’
Need for an ‘agreement’ to conduct transaction by electronic means

• UETA only applies to “transactions between parties each of which has agreed to conduct transactions by electronic means.”
• The agreement can be inferred – it is to be “determined from the context and surrounding circumstances, including the parties’ conduct.” UETA § 5(b)
• UETA § 6(1) provides that it is to be “construed and applied ... to facilitate electronic transactions consistent with other applicable law.” UETA § 6, Comment 2 explains that UETA was drafted “to permit flexible application consistent with its purpose to validate electronic transactions.”
• E-SIGN does not require any affirmative agreement, implied or otherwise. It specifies that it “does not require any person [other than governmental agencies in certain contexts] to agree to use or accept” E-Records or E-Signatures.
• As a matter of practice, an affirmative agreement (similar to UETA) is often obtained when there is reliance on E-SIGN
Examples of inferred agreement

• That agreement can be inferred from the context, including the parties’ conduct.
• The use of an onscreen form or a fax or PDF generally should suffice, at least if both parties use it. But what if an offer is made on paper but accepted via email – has the offeror “agreed” to conduct the transaction bound?
• It's better to have an express statement of agreement, such as the following immediately and prominently above the "I agree and submit" button:
  • By [clicking/tapping] the "[I agree and submit]" button below, I [we] agree (i) to enter into this Credit Line Review (including the agreements contained in it) electronically, (ii) to receive electronic statements concerning my account, and (iii) to the terms and conditions of the Credit Line Review (including the agreements contained in it).
• This indicates that both the party who prepared the text and the party who responds in the specified manner agreed to effect the contract by electronic means.
Scope: UCC Exclusion

- UETA and E-SIGN do not apply to the UCC, except for Articles 2 (sales of goods) and 2A (leasing of goods).
- Article 1 definition of “signing” (§ 1-201(b)(37)) and Article 9 definition of “authenticate” (§ 9-102) anticipate use of electronic signatures.
- But Article 1 definitions of “writing” and “written “(§ 1-201(b)(43)) still call for something reduced to “tangible form.”
- Article 3 requires a writing (see definition of ‘promise’ in § 3-103) for a note to be a ‘negotiable instrument’, so no electronic signatures are possible for a negotiable instrument, except for ‘transferable records’ subject to UETA or E-SIGN.
- Pending review of UCC to update for emerging technologies
Scope: real property transactions

- UETA an E-SIGN apply to an agreement concerning real estate between the parties
- Effect on third parties through recording may require paper documents
Scope: other exclusions

- Wills and the like
- Uniform Law Commission has just approved a uniform law on electronic wills
Scope: Entity actions

- Entity laws typically govern electronic signing of resolutions and the like.
- E.g., Delaware GCL §§ 141 (written consent of directors), 228 (written consent of shareholders), and 232 (notice to shareholders and definition of electronic transmission).
- See also, Delaware LLC Act §302; Delaware RUPA §407; Delaware RULPA §§ 302 and 405, and Delaware Statutory Trusts Act §3806(f)(2).
- UETA also validates matters (such as resolutions) that “relate” to transactions. UETA, § 2, Comment 13.
- Delaware entity acts amended effective August 1, 2019 broadening use of electronic signatures for entities (Delaware RUPA § 124, RULPA § 113, LLC Act § 113, GCL § 116).
What is an ‘electronic signature’?

• UETA and E-SIGN define “electronic signature” to mean “an electronic sound, symbol, or process, attached to or logically associated with a [In E-SIGN only: contract or other] record and executed or adopted by a person with the intent to sign the record.’

• An E-Signature thus includes:
  • A person typing his or her name on an e-mail or on the screen;
  • Clicking/tapping on a computer/device screen button that says "I agree", "Submitted", or equivalent language as long as the language demonstrates an intent to enter into an agreement; or
  • Manually signing a piece of paper and then sending an image of that piece of paper by electronic means (e.g., fax, PDF).
What is an ‘electronic record’?

- UETA and E-SIGN define ‘electronic record’ to mean ‘a [In E-SIGN only: contract or other] record created, generated, sent, communicated, received or stored by electronic means.’
- Both define ‘record’ to mean ‘information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form’
- UETA § 2, Comment 6 explains that “information stored on a ... disc, facsimiles, voice mail messages, messages on a telephone answering machine, audio and video tape recordings, among other records, all would be electronic records under this Act.”
Proving an E-Signature

• While UETA and E-SIGN enable the use of E-Signatures and E-Records in a broad range of circumstances, “other law” still applies to determine whether the record or signature is effective or, in the words of UETA, “has legal consequences.”
  • Similarly, E-SIGN specifies that it does not “limit alter or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons [thereunder] ... other than a requirement that contracts or other records be written, signed or in nonelectronic form.”
• How to show that a “signature” was the act of the person who purportedly signed it:
  
  **UETA Section 9. Attribution and Effect of Electronic Record and Electronic Signature.**
  
  (a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.
  (b) The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties’ agreement, if any, and otherwise as provided by law.
• Examples
Retention of E-Records by recipient

• Under UETA, § 8, if other law requires a person to “provide, send or deliver information in writing,” that requirement is satisfied if the information is provided in an E-Record “capable of retention by the recipient at the time of receipt.”
  • This does not mean that the recipient needs to actually retain the record.
  • But the sender cannot inhibit the ability of the recipient to store or print it. If the sender does so, “the electronic record is not enforceable against the recipient.” (emphasis added)
  • This is consistent with the above referenced definition of a “record,” which requires that it be “retrievable in perceivable form.”

• E-SIGN §101(e) is similar, but rather than addressing retainability by the recipient, it addresses retainability by those “entitled to retain” the contract or record. It provides that, if other law requires a record relating to a transaction to be in writing, “the legal effect, validity or enforceability of an electronic record may be denied if [it] is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.” (emphasis added)
  • E-SIGN does not address who is entitled to retain such a contract or record, and since neither common law nor the Statute of Frauds generally do not entitle anyone to retain a copy of a contract, this requirement may be of limited practical effect outside the realm of consumer protection or similar laws and regulations.
RetentionPolicy by sender

• Conversely, UETA § 12 provides that if a law requires that a record be retained, that requirement is satisfied by an electronic record that
• “accurately reflects the information set forth in the record after it was first generated in final form as an electronic record” and also
• “remains accessible for later reference.”

• E-SIGN §101(d)(1) contains a similar provision but requires that the information in the E-Record “remain accessible to all persons who are entitled to access” under the other law “in a form that is capable of being accurately reproduced for later reference.”

• As with the retainability provision in §101(e), E-SIGN does not address who is entitled to such access, effectively leaving that to other law
Delivery of Information to Consumers

• E-SIGN 101(c)(1) contains a complex and demanding consent requirement that must be satisfied before E-Records can be used to provide information (e.g., deliver disclosure materials) to consumers when, under other law, that information is required to be provided or made available in writing. Such consents must be affirmative, must be given after the consumer has received a clear and conspicuous disclosure of various enumerated rights, options and requirements relating to electronic delivery, and must be self-validating in the sense that the consent itself must be given “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.” (emphasis added)

• For example, if a disclosure is going to be provided by posting on the sender’s website, the consumer may need to provide his or her consent by accessing a page on that website.

• Failure to satisfy this requirement will mean that the required information will not be deemed to have been provided. But §101(c)(3) specifies that a failure to satisfy the “reasonable demonstration” test will not affect the “effectiveness, validity, or enforceability of any contract executed by a consumer.”

• Under E-SIGN §104(d)(1), Federal regulatory agencies are permitted to adopt rules exempting particular categories or types of records from the §101(c) consumer consent requirements, but only if such exemption is “necessary to eliminate a substantial burden on electronic commerce and will not increase the material risk of harm to consumers.”
Formation of agreements online

- No governing statute (as with UETA and E-SIGN)
- General rules of contract law apply
  - Courts adapt them to online context
- *Specht* and following decisions
- *Business Lawyer* article (‘Browse-Wrap Agreements …’, 2003)
  - Adequate notice of existence of the proposed terms
  - Meaningful opportunity to review the terms
  - Adequate notice that taking a specified action manifests assent to the terms
  - User takes that action
- *Draft*, Restatement of the Law, Consumer Contracts
  - Reasonable notice requirements
  - Page lay out
  - Clarity that manifesting assent creates a binding contract
Adding and modifying terms online

• ProCD and pay now terms later (PNTL)
• Difference when original agreement retains right to modify
• Role of good faith
• Opt out rights
• Effect on original agreement
Electronic Agents/Smart Contracts

- UETA and E-SIGN anticipate the use of smart contracts by enabling the formation of contracts without direct human involvement through the functioning of “electronic agents” that independently “initiate or respond to electronic records or performances … without review or action by an individual.” (Should probably give a short definition of “smart contract”)
- E-SIGN §101(h) provides that “a contract or other record … may not be denied legal effect, validity or enforceability solely because its formation, creation or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound.”
- UETA §14 is similar but more detailed. It specifies that a contract may be formed by the interaction of electronic agents “even if no individual was aware of or reviewed the electronic agents’ actions or the resulting terms and agreements.”
  - It also enables “click-through” or similar contracts formed through the interaction of an electronic agent for one party and an individual who is or acts for the other, so long as the individual knows that its actions (which must be voluntary) “will cause the electronic agent to complete the transaction or performance.”
- As with E-Signatures, however, it is necessary to be able to attribute the actions of an electronic agent to an actual party. This includes not only identifying the party but also attributing the requisite intent to that party.
  - As explained in UETA § 14, Comment 1 the “requisite intention” for the actions of a machine “flows from the programming and use of the machine.”
Special Statutory Requirements in Delaware Governing Entity Actions — Corporations

• “Electronic transmission” means any form of communication not directly involving the physical transmission of paper, that creates a record that may be retained, retrieved and reviewed by a recipient thereof, and may be directly reproduced in paper form by such recipient in paper form through an automated process. DGCL §232(c)

• Written consent of Board members may be made by electronic transmission if such consents are filed with the minutes in paper form (if the minutes are maintained in paper form) or electronically (if the minutes are maintained in electronic form). DGCL §141(f)

• Written consent of a Shareholder shall be deemed written, signed and dated for purposes of DGCL §228 if delivered with information from which the corporation can determine:
  • that the electronic transmission was transmitted by the shareholder/proxy holder/other authorized person, and
  • the date of the transmission (which shall be deemed the date the transmission was signed).

• Under DGCL §228(d)(1), unless otherwise provided by resolution of the board, no written consent of a Shareholder by electronic transmission shall be deemed to have been delivered until
  • the consent is reproduced in paper form, and
  • such paper form is delivered to the corporation by delivery to its registered office, to its principal place of business, or to an authorized officer or agent of the corporation who has custody of the minute books.

• Notices to shareholders may be given by a form of electronic transmission consented to by the shareholder to whom the notice is given (e.g., to a fax number or email address at which the shareholder has consented to receive notice). DGCL § 232
Special Statutory Requirements in Delaware Governing Entity Actions — LLCs, GPS, LPs, Statutory Trusts

• Each of these statutes has adopted a definition of electronic transmission identical to the definition contained in DGCL §302(c) (see references above).

• Each of these statutes permits consents delivered by electronic transmission to be deemed signed and delivered for purposes of the statute, “unless otherwise provided” in the operating agreement of the entity.
NOTE ON THE EXECUTION OF A DOCUMENT USING AN ELECTRONIC SIGNATURE

1. Introduction

This note has been prepared by a joint working party of The Law Society Company Law Committee and The City of London Law Society Company Law and Financial Law Committees (the JWP). This note has been developed to help parties (and their legal advisers) who wish to execute commercial contracts using an electronic signature or who wish to enter into a commercial contract with one or more other parties that intend to execute that contract using an electronic signature. The JWP has obtained legal advice from Leading Counsel (Mark Hapgood QC) on the use of electronic signatures as a valid method of executing documents. This note has been approved by Leading Counsel.

This note is limited in scope to commercial contracts entered into (and certain other documents signed) in a business context, rather than those to which consumers or other individuals outside of a business context are a party. However, it is recognised that certain of the principles considered in this note may also be applicable to documents entered into in other contexts. Each transaction should be approached according to its own facts and should take into account the wider implications of the transaction, including any relevant regulatory or tax implications.

This note is limited to the position under English law (the position under the laws of other parts of the United Kingdom may be different). See paragraph 7 of this note for a short discussion of when English law may not be the applicable law for determining whether or not a contract has been properly executed. Paragraph 8 of this note sets out a number of practical considerations which should be taken into account when considering whether to use an electronic signature.

2. Background

At present, where the parties to a transaction are not physically at the same meeting to sign the documents, it is common for the lawyers involved to arrange a signing via email, following the procedures set out in an earlier guidance note. This typically involves the signatory signing a hard copy document in wet ink, converting the document and signature into electronic form (e.g. by scanning or photocopying it) and sending it by email. However, as market practice and technology evolve, the use of electronic signatures is becoming increasingly common in a range of commercial transactions and that trend is expected to continue. Electronic signatures can take a number of different forms, including:

(a) a person typing his or her name into a contract or into an email containing the terms of a contract;

(b) a person electronically pasting his or her signature (e.g. in the form of an image) into an electronic (i.e. soft copy) version of the contract in the appropriate place (e.g. next to the relevant party’s signature block);

(c) a person accessing a contract through a web-based e-signature platform and clicking to have his or her name in a typed or handwriting font automatically inserted into the contract in the appropriate place (e.g. next to the relevant party’s signature block); and

(d) a person using a finger, light pen or stylus and a touchscreen to write his or her name electronically in the appropriate place (e.g. next to the relevant party’s signature block) in the contract.

This note does not focus on any one method of electronic signature, but rather on setting out the principles for determining whether a given document signed with an electronic signature has been validly executed.

---

1 Note on Execution of Documents at a Virtual Signing or Closing prepared by a joint working party of The Law Society Company Law Committee and The City of London Law Society Company Law and Financial Law Committees in May 2009.
3. **Legislative framework**

Regulation (EU) No 910/2014 (the **eIDAS Regulation**) has direct effect in EU Member States from 1 July 2016.\(^2\) It establishes an EU-wide legal framework for electronic signatures (as well as for electronic seals, electronic time stamps, electronic registered delivery services and website authentication, all of which are outside the scope of this note).

The eIDAS Regulation defines:

(a) an “**electronic signature**” as “data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign”;

(b) an “**advanced electronic signature**” as one which meets the following requirements: (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; and

(c) a “**qualified electronic signature**” as “an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures”.

Articles 25(2) and (3) of the eIDAS Regulation provide that a qualified electronic signature shall have the equivalent legal effect of a handwritten signature and that a qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States. However, Article 25(1) of the eIDAS Regulation also provides that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures. Furthermore, Recital 49 of the eIDAS Regulation states that (apart from the requirements for qualified electronic signatures) it is for national law to define the legal effect of electronic signatures.

As at the date of this note, qualified electronic signatures are not commonly used in England. Therefore, neither the concept of a qualified electronic signature nor the provisions of Articles 25(2) and (3) of the eIDAS Regulation have been relied on in reaching the conclusions set out in this note.

The Electronic Communications Act 2000 (the **ECA 2000**) provides a statutory framework for the admissibility of electronic signatures in England and Wales. Section 7(1) of the ECA 2000 provides that in any legal proceedings (a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and (b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity or integrity of the communication or data. Although the ECA 2000 deals with the admissibility of electronic signatures, it does not deal with the validity of electronic signatures. The conclusions about the validity of electronic signatures set out in this note are therefore based on wider principles of English common law.

In addition, Section 8 of the ECA 2000 provides for the UK government to modify by statutory instrument (\(\text{SI}\)) any enactment which requires something to be done or evidenced in writing, to be authorised by a person’s signature or seal or to be delivered as a deed or witnessed. Although more than 50 such SIs have been enacted under the ECA 2000, there are many statutory provisions imposing execution formalities which have not been addressed in this manner. However, in the opinion of Leading Counsel and the JWP, the fact that an SI has not been enacted under the ECA 2000 in respect of a particular statutory provision imposing an execution formality does not mean that a contract subject to such provision cannot be executed using an electronic signature (and this is supported by the eIDAS Regulation).

---

4. Using electronic signatures to execute English law governed documents

4.1 Simple contracts

In the absence of any (usually statutory) requirement, there is no need under English law for contracts to be in any particular form; in fact they can be entered into orally, provided there is offer and acceptance, consideration, certainty of terms and an intention to be legally bound. Therefore, a simple contract may be concluded using an electronic signature.

4.2 Documents subject to a statutory requirement to be in writing and/or signed and/or under hand

A number of types of document are subject to specific formalities imposed by statute, including a requirement for the document to be in writing and/or signed and/or under hand. Examples include:

(a) Section 4 of the Statute of Frauds 1677 requires a guarantee or a memorandum or note thereof to be in writing and signed by the guarantor or some other person authorised by the guarantor to do so;

(b) Section 2 of the Law of Property (Miscellaneous Provisions) Act 1989 (the LP(MP)A 1989) requires a contract for the sale or other disposition of an interest in land in England and Wales to be in writing and signed;

(c) Section 53(1) of the Law of Property Act 1925 (the LPA 1925) requires a disposition of an equitable interest to be in writing, signed by the person disposing of it or by his properly authorised agent;

(d) a statutory assignment within Section 136 of the LPA 1925 must (among other requirements) be in writing and signed by the assignor;

(e) under Section 83 of the Bills of Exchange Act 1882, a promissory note must (among other requirements) be in writing and signed by the maker;

(f) under Section 90(3) of the Copyright, Designs and Patents Act 1988, an assignment of copyright is not effective unless it is in writing signed by or on behalf of the assignor; and

(g) under Section 1(1) of the Stock Transfer Act 1963, registered securities may be transferred by means of an instrument under hand in the form set out in Schedule 1 to the Act.

In the opinion of Leading Counsel and the JWP, a contract executed using an electronic signature (and which may exist solely in electronic form) satisfies a statutory requirement to be in writing and/or signed and/or under hand for the following reasons.

(i) Writing: The Interpretation Act 1978 defines “writing” to include “typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form”. Where the contract is represented on a screen (including a desktop, laptop, tablet or smartphone) in a manner which enables a person to read its terms properly, it will be “in writing” at that point. For example, in Golden Ocean Group Limited v Salgaocar Mining Industries Pvt Ltd and another [2012] EWCA Civ 265 (Golden Ocean), the Court of Appeal found that the exchange of a number of emails could lead to the conclusion of an agreement in writing for the purposes of the Statute of Frauds 1677.
(ii) **Signature:** The test for determining whether or not something is a signature is whether the mark which appears in a document was inserted in order to give, and with the intention of giving, authenticity to it. Therefore, provided that the signatory inserts an electronic signature into the appropriate place (e.g. next to the relevant party’s signature block) in a document with the intention of authenticating the document, a statutory requirement for that document to be signed will be satisfied. It does not matter how the signatory inserted the electronic signature into the document (e.g. using any of the methods specified in paragraphs 2(a)-(d) above), nor does it matter in what form that signature was inserted (e.g. a handwritten signature, a generic handwriting font, a typed font, etc.). Leading Counsel has advised that *J Pereira Fernandes SA v Mehta [2006] EWHC 813 (Ch)* is authority that typing a name into an email satisfies a statutory requirement for a document to be signed (and this position was confirmed in *Green (Liquidator of Stealth Construction Ltd) v Ireland [2011] EWHC 1305 (Ch)*) and Golden Ocean is authority that an electronic signature has the same legal status as a wet ink signature, the key question being whether or not the purpose of the signature is to authenticate the document.

(iii) **Under hand:** A document is generally understood to have been executed under hand if it has been executed otherwise than by deed. The insertion of an electronic signature with the relevant authenticating intention would be sufficient for a document to have been executed under hand.

### 4.3 **Deeds**

At common law, a deed must be in writing. Given the willingness of the courts to interpret various statutory requirements for writing to include the situation where a document is represented on a screen and executed with an electronic signature, in the opinion of Leading Counsel and the JWP, the approach outlined above would apply in respect of deeds. For the execution of deeds:

(a) **Section 46 of the Companies Act 2006 (the CA 2006)** provides that a document is validly executed as a deed by a company incorporated under the CA 2006 if it is duly executed and is delivered as a deed.

(i) **Section 44 of the CA 2006** provides that one of the ways in which a document can be validly executed by a company incorporated under the CA 2006 is by signature by two directors or by one director and the company secretary (authorised signatories). In the opinion of Leading Counsel and the JWP, this can be achieved by each of two authorised signatories signing the deed (using an electronic signature or another acceptable method) either in counterpart or by one authorised signatory signing, followed by the other adding his or her signature to the same version (electronic or hard copy) of the deed.

(ii) **In the opinion of Leading Counsel and the JWP,** delivery can be achieved through electronic signing, but the parties will have to take steps to ensure the signing arrangements adequately address when delivery takes place, particularly if the parties propose that their lawyers hold their signed documents to the order of the relevant party prior to the deed coming into effect.

(b) **Section 1(3) of the LP(MP)A 1989** provides that an instrument is validly executed as a deed by an individual (including an individual acting under a power of attorney) if it is signed by him in the presence of a witness who attests the signature (and, by Section 1(4), “sign” includes making ones mark on the instrument). Section 44 of the CA 2006 provides that another of the ways in which a document can be validly executed by a company incorporated under the CA 2006 is if it is signed on behalf of the company by a director of the company in the presence of a witness who attests the signature. In the opinion of Leading Counsel and the JWP, where a suitable signatory signs a deed using an electronic signature and another individual genuinely observes the signing (i.e. he or she has sight of the act of signing and is aware that the signature to which he or she is attesting is the one that he or she witnessed), he or she will be a witness for these purposes. If that witness subsequently signs the adjacent attestation clause (using an electronic signature or otherwise), that deed will have been validly executed. The practical means of witnessing different forms of electronic signature will need to be settled on a case-by-case basis, with consideration given to the evidential weight of the form agreed (see paragraph 5 below). However, in the opinion of Leading Counsel and the JWP, it is best practice for the witness to be physically present when the signatory signs, rather than witnessing through a live televisual medium (such as a video conferencing facility), in order to minimise any evidentiary risk as to whether the person genuinely witnessed the signing.
4.4 Companies incorporated under the CA 2006: minutes and resolutions

Leading Counsel has advised that:

(a) a document (including minutes of a directors’ meeting under Section 249 of the CA 2006 and a members’ written resolution under Section 296 of the CA 2006) signed with an electronic signature by a person and sent or supplied to a company will have been sufficiently authenticated for the purposes of Section 1146 of the CA 2006 if:

(i) it is sent or supplied in hard copy form by or on behalf of the person who signed it; or

(ii) it is sent or supplied in electronic form, provided that the identity of the sender is confirmed in a manner specified by the company or (where no such manner has been specified by the company) if the communication contains or is accompanied by a statement of the identity of the sender and the company has no reason to doubt the truth of that statement;

(b) minutes of the proceedings of a general meeting that are signed by the chairman using an electronic signature constitute evidence of the proceedings of that meeting in accordance with Section 356(4) of the CA 2006 and a record of a resolution passed otherwise than at a general meeting that is signed by a director or the company secretary using an electronic signature constitutes evidence of the passing of that resolution in accordance with Section 356(2) of the CA 2006; and

(c) the directors of a company that has adopted the CA 2006 Model Articles for private companies limited by shares, the CA 2006 Model Articles for public companies limited by shares or the Companies Act 1985 Table A articles may take a decision or pass a directors’ written resolution (as applicable) under those articles by the relevant directors signing a resolution using an electronic signature.

4.5 Using a combination of execution methods

If one (or some) parties to a document (including any witnesses) wish to sign using an electronic signature, while another (or others) would prefer to use another acceptable method (e.g. a wet-ink signature), there is no reason why the document cannot be signed using a combination of different methods, so long as each party uses a valid signature method, although there may be practical advantages (e.g. electronic storage) if a document is created only in an electronic process.

5. Evidential weight

Section 7 of the ECA 2000 provides that in any legal proceedings, an electronic signature incorporated into a particular electronic communication shall be admissible in evidence in relation to any question as to the authenticity of that communication or as to the integrity of that communication. Leading Counsel has advised that, if the authenticity of a document signed using an electronic signature were to be challenged, an English court would accept the document bearing the electronic signature as prima facie evidence that the document was authentic and, unless the opponent adduced some evidence to the contrary, that would be sufficient to deal with the challenge. These are the same principles that an English court would apply in relation to wet-ink signatures.

The person alleging that the document was not authentic (e.g. produced fraudulently, not signed by the person who had purportedly done so or not properly witnessed) would need to prove, on a balance of probabilities, that this was the case. The Code of Conduct of the Solicitors Regulation Authority provides that a solicitor should not allege fraud without material which he or she reasonably believes shows, on the face of it, a case of fraud. Under the Bar Standards Board Code of Conduct it is necessary to have reasonably credible material which establishes an arguable case of fraud before a barrister can plead fraud. Although it would not (in the absence of handwriting) be possible to adduce evidence of a handwriting expert, there is a spectrum of evidence that might be used to prove the authenticity of a particular signature. It may be possible, for example, to show (i) that the purported signatory or witness accessed the electronic document via his or her email account or computer, (ii) the location in which it was accessed, (iii) that he or she used a password and/or PIN or encryption key in order to access the document (if that was the case), (iv) the time at which he or she applied his or her signature; and/or (v) that the document had not been amended between when it was uploaded to the electronic signature platform and when the final signatory executed it.
On certain transactions solicitors may be involved in checking the identity of a signatory, the authenticity of a signature and/or the question of whether or not a document has been properly approved. On other transactions the identity, authenticity and approval may be assumed. The use of electronic signatures will not change this.

6   **Originals and counterparts**

Leading Counsel has advised that:

(a) it is possible, depending on the facts, to have multiple originals of a document in both electronic and hard-copy form (including, for example, where the parties intend for multiple originals to be produced in electronic and/or hard-copy form), but it would not be appropriate if it would conflict with other legal requirements (as would be the case with, for example, promissory notes);

(b) where a document has been executed electronically with each signatory applying his or her signature to the same file uploaded to the relevant electronic signature platform, the signatories will be deemed to have signed the same counterpart;

(c) where a document has been executed electronically, there is no need as a matter of English law for an additional wet-ink version to be executed, although there may be practical reasons for doing so (see paragraphs 7(b) and 8(d));

(d) where a document has been executed using a combination of electronic and wet-ink signatures, the parties or their legal advisers may wish to create a composite document (either by using a hard-copy print out of the electronically-signed document and the wet-ink signed pages or by scanning the wet-ink signed pages and creating a composite electronic document) and to the extent that the document is required to be produced in evidence, an English court would accept this composite document;

(e) to the extent that an original of a document executed electronically is required to be produced in evidence, an English court would accept an electronic version of that executed document or a hard-copy print out;

(f) where an undated document is executed electronically, it may be validly dated with the authority of the parties (i) by inserting the date electronically or (ii) by printing it out and inserting the date by hand; and

(g) after a document has been executed electronically, amendments may be made to it (electronically or in manuscript) to the same extent as amendments may be made in manuscript to a document executed in wet ink.

7.   **Conflicts of law issues**

In certain circumstances, the parties to a document to be signed using an electronic signature may wish to seek advice from counsel in another jurisdiction. For example:

(a) **Where a document governed by English law is to be executed by an overseas company**:3

   (i) In any litigation in the English courts, the courts will be obliged to apply Article 11 of Regulation (EC) No 593/2008 on the law applicable to contractual obligations (the *Rome I Regulation*) to determine questions as to which law should be applied to ascertain whether or not a contract is formally valid (assuming it is a civil and commercial matter and its subject matter is not excluded from the *Rome I Regulation*). Article 11 of the *Rome I Regulation* provides that one of the ways in which a contract is formally valid is if it satisfies the formal requirements of the law which governs it (although this rule does not apply to consumer contracts and there are specific provisions to be considered for contracts concerning rights in rem in immovable property and for tenancies of immovable property). Therefore, for matters within the scope of the *Rome I Regulation* in any action brought in the English courts, a contract governed by English law will be upheld as validly executed so long as it has been validly executed as a matter of English law.

3 i.e. a company which is not incorporated under the CA 2006.
(ii) Section 44(1) of the CA 2006, as modified by the Overseas Companies (Execution of Documents and Registration of Charges) Regulations 2009, provides that, as a matter of English law, a document (including a deed) can be validly executed by an overseas company (x) by the affixing of the company’s common seal; (y) if it is executed in any manner permitted by the laws of the territory in which the company is incorporated for the execution of documents by such a company; or (z) if it is signed by a person who, in accordance with the laws of the territory in which the company is incorporated, is acting under the authority (express or implied) of the company and it is expressed (in whatever form of words) to be executed by the company.

(iii) Therefore, if an overseas company executes an English law governed contract using an electronic signature, provided that the relevant signatory is (as a matter of the laws of the territory in which the company is incorporated) acting under the authority (express or implied) of the company, that contract will have been validly executed as a matter of English law. The question of the authority of a signatory, including any limitations on the scope of that authority and the manner in which the company binds itself (i.e. whether signature by electronic means is excluded), is a matter of the laws of the territory in which the company is incorporated (as is the question of that company’s capacity).

(b) Where any litigation, or other action, in relation to a document governed by English law may take place, or be required, outside England: Examples include where (i) there is a foreign jurisdiction clause in an English law contract, (ii) an English judgment needs to be enforced in another jurisdiction, (iii) a claim needs to be made in a non-English insolvency proceeding, (iv) a document needs to be notarised or apostilled and (v) a registration needs to be made at a non-English registry. In such circumstances, parties may wish to seek local law advice in advance of signing by electronic signature. Where such action may take place elsewhere in the European Union, parties may wish to consider the feasibility of using a qualified electronic signature (see paragraph 3 of this note).

(c) Where a document is governed by a law other than English law: Whether or not such a document can be validly executed using an electronic signature and the steps required in order for such an execution to be valid are matters of the governing law and, in some jurisdictions, the impact of the law of the forum where the document is relied upon and are beyond the scope of this note.

8. **Certain other considerations**

This note is limited to the question of whether or not an electronic signature can be used to validly execute a commercial contract as a matter of English law. However, where one or more parties to a contract are contemplating using an electronic signature, there are a number of other legal and practical matters which they or their legal advisers might need to consider, including the following.

(a) Does an entity intending to execute the contract using an electronic signature have the corporate capacity and authority to do so? This will depend on the facts, but should not differ from the position where the party is executing the contract with a pen, unless there is something in its constitutional documents or board resolutions restricting it from using an electronic signature. In the absence of any specific restriction, it is not necessary to include a reference to electronic signature in any board resolution or for the constitutional documents to specifically reference the fact that the entity can enter into agreements or transactions which are signed electronically.

(b) Is there sufficient certainty that the person purporting to sign using an electronic signature is in fact that person or acting under the authority of that person? Factors that might assist in this respect include (in particular, where the contract has been executed through an e-signing platform) whether the signatory had accessed the document using a particular email address or by inputting a unique access code and whether or not this can be confirmed (via a certificate or otherwise) by the platform provider.

(c) Is the document to be distributed, signed and held electronically in a manner which is sufficiently secure? This will depend on the method used and on the degree of importance placed on IT security by the parties in question (for example, how valuable is the contract; how important is it to keep it confidential?), so it is something that each party should consider on a case-by-case basis and draw its own conclusions.
(d) Where the document needs to be filed with an authority or registry, will that authority or registry accept electronic signatures? For example, as at the date of this note:

(i) the Land Registry and the Land Charges Registry require a wet-ink signature on a paper version of any document submitted to them for registration (although the Land Registry has announced plans to launch an electronic mortgage service);

(ii) Companies House will accept a certified copy of a charging document executed using an electronic signature in satisfaction of the registration requirements under Section 859A of the CA 2006 (although, outside of its web-filing service, it still requires a wet-ink certification of the copy); and

(iii) where stamp duty is payable on a document, H.M. Revenue & Customs would normally expect to stamp a version of the document with a wet-ink signature.

(e) If the place of signature or the location of the document has particular legal consequences (e.g. in relation to the payment of stamp duty), where will a document executed using an electronic signature be treated as having been executed or located? The answer may depend upon a number of factors, including where the signatory is physically located when signing and where the server on which the document is stored is located. In such circumstances, it may be better to have a physical signing.

(f) Where a party wishes to execute a deed by the physical affixing of its common seal, it is unlikely to be possible to do this electronically (although the eIDAS Regulation and the ECA 2000 provide for the creation and use of electronic seals, these are not, so far as the JWP is aware, currently in use in England).

(g) It is not necessary to include any specific reference to electronic signatures in the document itself in order for it to be validly executed using an electronic signature.

This note refers to certain EU regulations, the status of which under English law may be affected by the United Kingdom ceasing to be a member of the European Union.

The Joint Working Party

13 July 2016

DISCLAIMER:

This note was developed by a joint working party of the Law Society Company Law Committee and the City of London Law Society Company Law and Financial Law Committees and has been approved by Leading Counsel. The aim of this note is to make suggestions only and not to give advice. No duty of care or liability whatsoever is accepted by those involved in the preparation or approval of this note, or the firms or organisations that they represent, to any company or individual who relies on material in it.