A global overview of electronic signatures

An *electronic signature*—also known as an "*e-signature*"—is a simple and legally recognized way to indicate consent or approval on a digital document or form. Since countries may have differing laws when it comes to e-signatures, international companies, including U.S. and European companies that do business abroad, must consider e-signature laws on a global scale. The good news is that e-signatures are legally valid and enforceable in nearly every industrialized country around the world. But how can companies effectively use e-signatures no matter where they do business?

This white paper explores the current landscape of global e-signatures laws to help your company understand how to use electronic signatures internationally.

Types of electronic signatures

E-signatures are legally binding in nearly every industrialized nation, and even less developed countries are beginning to enact e-signature laws. Worldwide, there's a difference in how experts use the terms "electronic" signatures and *"digital" signatures*.

Electronic signatures

An electronic signature is generally any electronic process that indicates acceptance of an agreement or form. A range of methods can be used to authenticate the identity of participants, including email addresses, Enterprise IDs, phone authentication, knowledge-based authentication and passwords. In addition, many electronic signature solutions offer workflows that track every step in the signature process, such as when the agreement was sent, opened, and signed, as well as the IP and email address of each signer or approver. The best of these solutions capture this additional data in a secured audit trail, which provides clear, easily producible evidence of each party's signature.

Digital signatures

A digital signature is a specific type of electronic signature that requires the signer to authenticate their identity using a certificate-based digital ID. The digital certificate is generally issued by an independent Certificate Authority (CA), which verifies the identity of the signer before issuing the certificate. In some jurisdictions, like the European Union, a distinction is made between two types of electronic signatures that are typically implemented using certificates: Advanced Electronic Signatures (AdES) and Qualified Electronic Signatures (QES). While both are uniquely linked to the signer, the latter requires that participants use Qualified Certificates issued by accredited CA's as well as a qualified signature creation device (QSCD) signature creation device, such as a smart card, USB token, or cloud-based trust service.

In addition to providing audit trails, solutions that work with digital signatures rely on the fact that the signed document itself can produce evidence of each participant's signature. During the signing process, the signer's certificate is bound to the document using the private key uniquely held by the signer. During the validation process, the reciprocal public key is extracted from the signature and used to both authenticate the signer's identity through the trusted CA and to confirm that no changes were made to the document since it was signed.

E-signatures vs. digital signatures

At a global level, both e-signatures and digital signatures can be used in legal signing processes, but the specific choice for your company will depend upon your unique regulatory environment, risk profile and business requirements. As an example, the world's two largest financial markets, the European Union and the United States, demonstrate a marked contrast in legal approaches. The EU distinguishes between types of electronic signatures and affords a clear preference for digital signatures. In contrast, US law allows for a

broader definition and is not prescriptive of specific technology. So, while digital signatures extend proof of signing to the document itself and offer an advanced form of authentication for signing processes, getting certificates for all participants adds cost and complexity to the solution and may limit your flexibility when it comes to working with customers or business partners. The right solution for your business will balance regulations and risk—and consider what level of effort is necessary to make your business transactions both legal and secure.

Types of electronic signature laws

Worldwide, there are generally three types of electronic signature laws:

- "Minimalist" or "permissive" laws allow for the broad enforceability of e-signatures with few legal restrictions.
- "Two-Tier" laws generally permit the use of electronic signatures but provide greater evidentiary weight to digital signatures.
- "Prescriptive" laws dictate specific technical methods to electronically sign a document, typically digital signatures.

Minimalist laws

With some exceptions, minimalist laws permit the use of electronic signatures for virtually all uses and are generally technology-neutral. For example, the Electronic Signatures in Global and National Commerce Act (ESIGN Act), the United States' electronic signature law, contains a general rule of validity, stating in part:

1. A signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
2. A contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

Although three different types of laws govern e-signatures worldwide, minimalist laws provide the widest protection and work in most situations. Where possible, it makes sense to update your agreements to select the governing law and venue of a country with minimalist laws, like the United States, Australia, New Zealand, and Canada, you can often use electronic signatures worldwide.

Two-Tier laws

Many countries have enacted a two-tier approach to legislation governing electronic signatures. This approach is a hybrid of minimalist and prescriptive laws. Two-tier laws accept all or most electronic signatures on a technology-neutral basis like minimalist laws, but they also create a class of approved technologies like prescriptive laws. The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures and the new European Union regulation on electronic identification and trust services (eIDAS) set to take effect in July 2016 are two-tier laws. It's important to keep in mind that even though these laws may dictate a specific process to create digital signatures, most of these countries also allow private parties to agree between themselves what will be an acceptable form of signature. This allows a good degree of flexibility in developing your contracting processes.

Most of the European Countries, China and South Korea have enacted two-tier electronic signature laws.

Prescriptive laws

Prescriptive laws are relatively rare. They require a specific technical method to electronically sign a document, and they dictate the types of signature technologies that are acceptable. Some prescriptive laws go so far as to deny the legal rights to an electronic transaction, unless they are secured using approved technology. Only a few countries have prescriptive e-signature laws, including Brazil, India, Israel, and Malaysia.

Effectively using electronic signatures worldwide

Although e-signature laws vary from country to country, you can develop a corporate e-signature policy that works worldwide. Where possible, your company can take advantage of minimalist laws by designating the governing law of a country with minimalist laws in its agreements. That means the agreement itself defines the e-signature laws that apply to it based on the specified governing law. Where required, you can comply with two-tier or prescriptive laws as needed, especially if your signature solution supports both e-signatures and digital signatures. For information on country-specific e-signature laws, refer to the *Global Guide to Electronic Signature Law*, which details the laws in over 45 countries across the globe.

Professional e-signature solutions, such as *Adobe Sign*, make it easy to set up agreements that work across multiple countries with just a few simple steps. You can use it to support business processes that require e-signatures, digital signatures, or a combination of the two. Workflow templates can include predefined disclosures or clauses for particular types of agreements, and you can automate approval workflows to route, track, and log every step of the process and then store signed documents in a searchable repository. You can also follow some best practices to help ensure your agreements are enforceable. For more information about best practices, read *Developing an Effective Electronic Signature Policy*.

For more information

To learn more about e-signature laws, policies, and solutions, consult these additional resources:

- *US Overview of Electronic Signatures*
- *Developing an Effective Electronic Signature Policy*
- *Global Guide to Electronic Signature Law*
- *Adobe Sign Solution Brief*

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

4/16