CIOReview

Raising the Bar for Legal Evidence of Valid E-Signatures

by Pem Guerry, EVP, SIGNiX

The signature is the foundation of commerce: it validates the execution of essential agreements, waivers and transactions. And now, as businesses and society adapt to today's omni-channel, mobile environment, this fundamental tool is going digital—organizations are increasingly forgoing handwritten signatures for electronic ones.

This pivot toward e-signatures is evidenced by the 53 percent average annual growth rate in the use of e-signatures since 2014, with nearly 700 million e-signed transactions expected in 2017, according to Forrester Research. The increasing use of mobile will only add to this trend.

As this growth and adoption has accelerated, e-signatures are no longer being confined to low-risk, low-volume transactions that hold little litigious danger. Even highly regulated industries are adopting e-signatures due to the many benefits to all parties.

"The technology not only improves mobility and efficiency but also better protects data and documents."

It's important for CIOs to note, however, that the e-signatures that seemed suitable for simple forms or low-risk contracts may not be appropriate for high-stakes transactions, like a mortgage document, legal contract or clinical trial submission form. The bar for e-signing these critical documents must be raised to assure documents and signatures are wholly and legally valid and will remain so in the future, and fortunately such alternatives are available.

Industry Requirements

A number of industries today have published guidelines on what types of e-signatures are permissible for certain transactions, such as the following:

- **Tax:** The Internal Revenue Service provides guidance for using e-signatures when executing various forms. Requirements include processes such as deploying knowledge-based authentication and recording a taxpayer's IP address for remote transactions.

continued on next page

• **Pharma/Life Sciences and Healthcare:** Organizations using e-signatures in the pharmaceuticals, life sciences or healthcare spaces may have to meet standards set forth by the U.S. Food and Drug Administration (FDA) and the Health Insurance Portability and Accountability Act (HIPAA). For instance, if submitting clinical trial documents to the FDA, organizations must comply with 21 CFR Part 11, which requires detailed audit trails, protection against document tampering and multi-factor identity authentication.

• **Financial Services:** Broker-dealers, financial advisors, bankers and others in the financial services industry must adhere to strict data privacy and cybersecurity measures.

• This list is far from exhaustive. There are other regulations for annuities, alternative investments, mortgages and other industries—as well as guidelines for consumer protection.

And for organizations doing business outside of the United States, there are other e-signature regulatory complexities to navigate. For example, the European Union is at the eve of a new regulatory era for electronic signatures. Regulation (EU) N°910/2014, on electronic identification and trust services for electronic transactions in the internal market (eIDAS), will soon become the European standard, and it will state new rules for using electronic seals, time stamping, validation and e-signatures.

Security Strongholds

So how can those charged with information, security and digital compliance meet these evolving requirements and ensure airtight e-signature legal evidence? This begins with the using the right foundational software and strategy.

There are several different kinds of e-signatures that organizations can use, but digital signatures, or independent e-signatures, consistently provide superior legal evidence. That's because digital signatures use secure public key infrastructure technology to permanently embed a signature's cryptographic information directly into a signed document. Users can verify signed documents online or offline, without relying on a vendor. When e-signatures don't use standards-based public key infrastructure, which is the case for many e-signature products, evidence is often bound to a vendor's server, where users must have an Internet connection and a relationship to a vendor to access it.

For these reasons, digital signature technologies based on robust and secure public key infrastructure, or PKI, is the most broadly supported e-signature technology worldwide. But CIOs must probe deeper into the technical and legal elements of e-signature solutions and practices to raise the bar for legal evidence as high as it needs to go.

•**Tamper-Evidence/Tamper-Proof Technology:** A document's long-term validity is severely threatened if there is no way to know that it wasn't altered after being signed. Document integrity can only be upheld with tamper-evident technology that captures, records, and alerts users to changes after each signature or initial is applied. Tamper-proof technology takes this principle to the next level—it prevents any changes to documents after signing.

continued on next page

Some e-signature services may only apply a tamper seal after all signatures have been applied to a document. But tread carefully. What happens if someone adjusts a contract provision after the first person signed, but the tamper seal isn't applied until the third person has signed? It opens a hole for anyone attempting fraud and for opposing legal counsel to deny the validity of the document.

- **Clear and Conspicuous Disclosures**: Many regulators, like the FTC, require "clear and conspicuous" disclosures that state a user's rights or options to make the signing process available on paper, how consent is applied, procedures to withdraw consent, how to request a paper copy of a record, etc. That is, your organization and/or e-signature provider must provide disclosures that are prominently placed (it can't be up to a signer to hunt for it) and in understandable language.

- **Identity Authentication:** For any type of transaction, organizations must have a way to validate signers' identities. This can be done through many different levels of identity authentication technology, from basic email-only verification to knowledge-based authentication to a combination of authentication methods. Some industry regulators require specific types of identity authentication. As a general rule, the more stringent the identity vetting, the more trusted and defensible the e-signature becomes.

- **Comprehensive Audit Trails:** E-signature evidence is of little use if the entire signing process is not well documented. An audit trail is essential to long-term validity, but they can vary wildly in the marketplace relative to the level of detail. It's important that audit trails consistently capture and record every element of the signing process—including document creation, document changes, the issuing of digital certificates, when every e-signature and initial is made and more.

As our world becomes more digital, the complexity and relevance of e-signatures will only grow. Raise the e-signing bar now and ensure the legal validity of your organization's documents and transactions in the future.