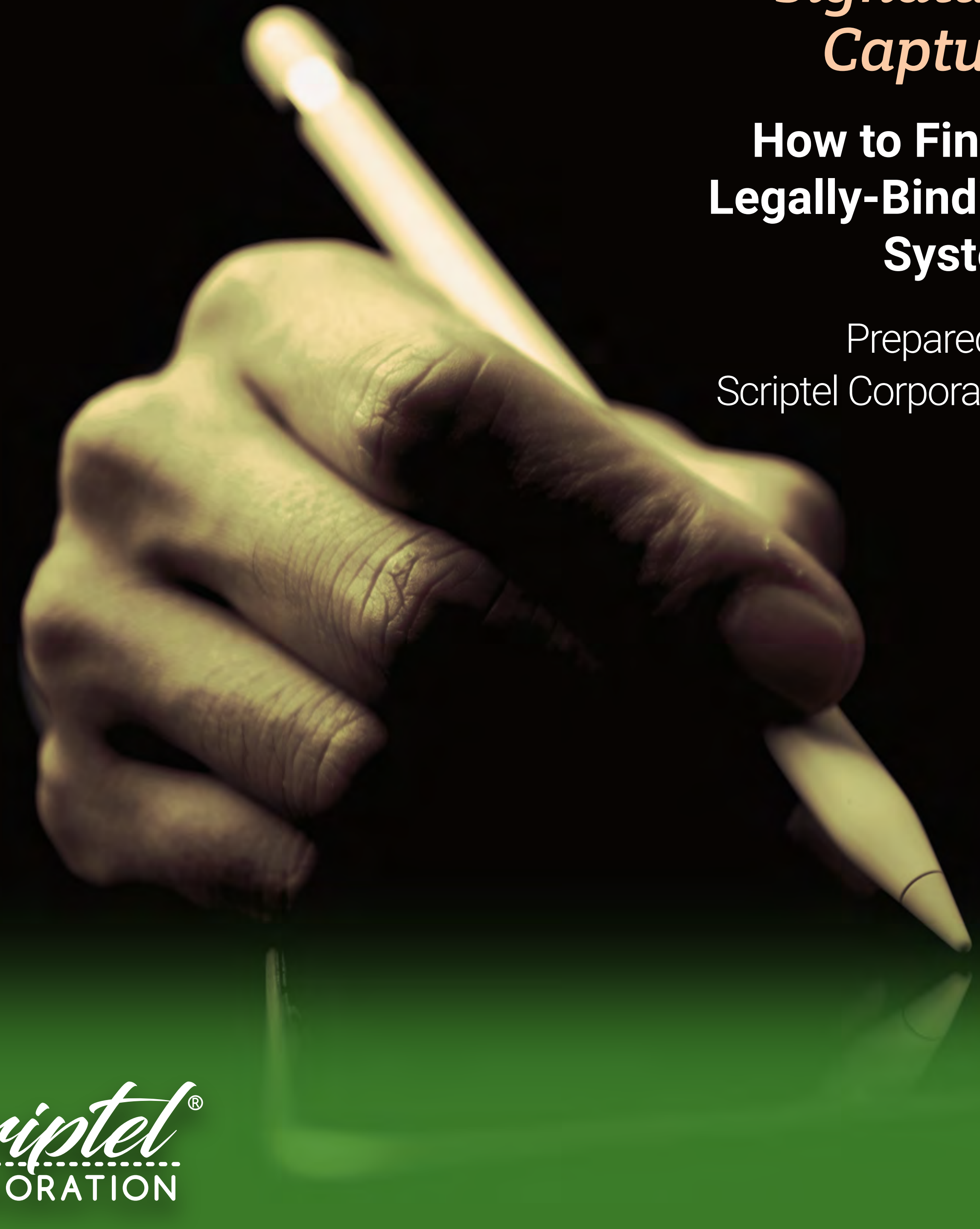
MARKETING WHITE PAPER

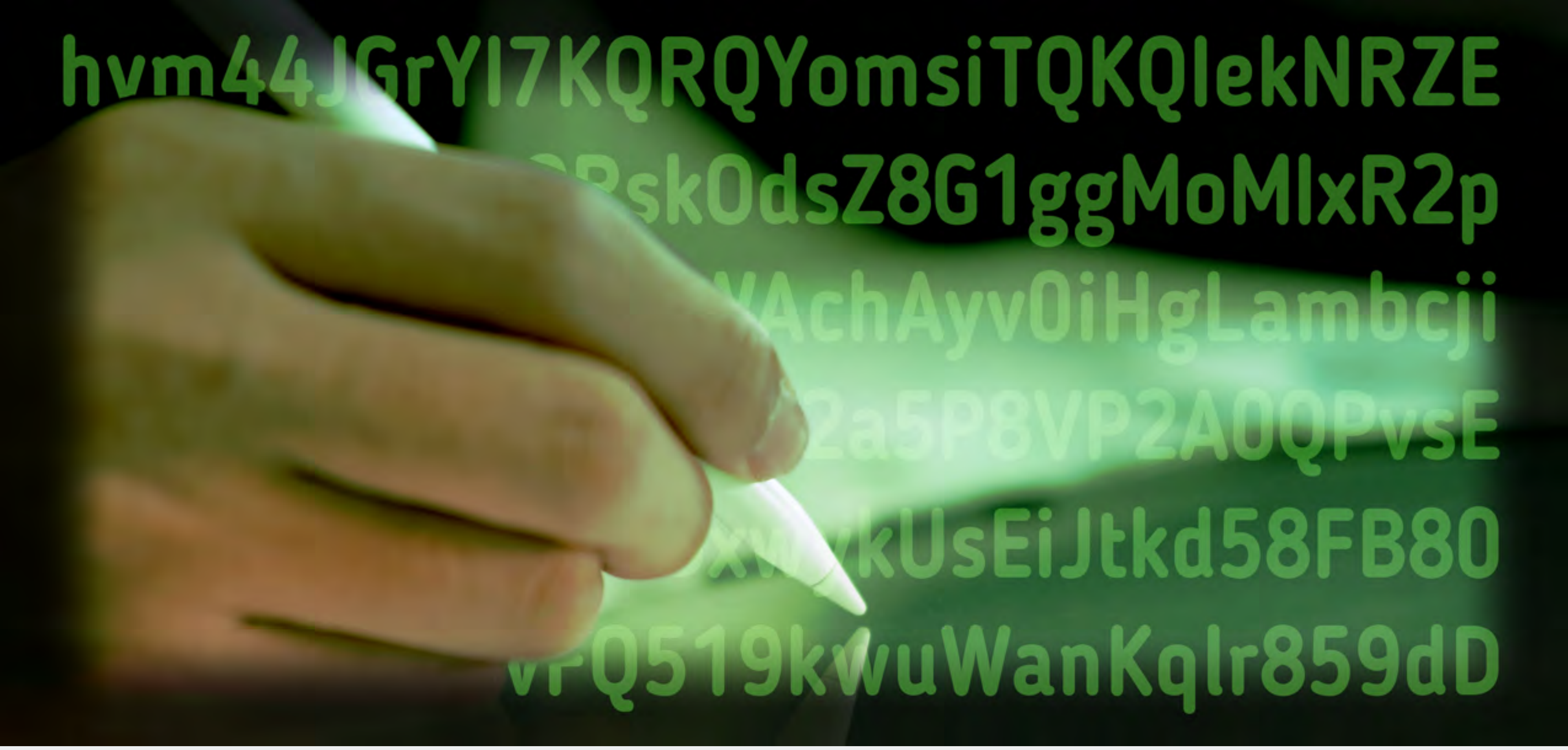
Understanding Biometrics and Electronic Signature Capture

How to Find a Legally-Binding System

Prepared by
Scriptel Corporation



Scriptel®
CORPORATION



Understanding the Use of Electronic Signatures

As businesses look to replace paper documents, contracts, and forms with more efficient digital substitutes, capturing signatures electronically becomes increasingly important.

Creating, signing, transmitting, and storing any and all documents in an electronic, legally-binding way seems like a daunting task, especially for small- to medium-sized businesses. This article will explain the electronic signature solutions available, and how to choose one that is the best fit.

What is a Legally-Binding Electronic Signature?

In the United States, electronic signatures are covered under the Uniform Electronic Transactions Act (**UETA**) and Electronic Signatures in Global and National Commerce (**ESIGN**) law. These two laws serve as the framework for electronic commerce implementation at the Federal level, and as the basis for most state-level e-commerce laws.

These laws specify a valid, electronic signature is a "sound, symbol, or process, logically associated with a document" with the following qualities:

Unique to each user

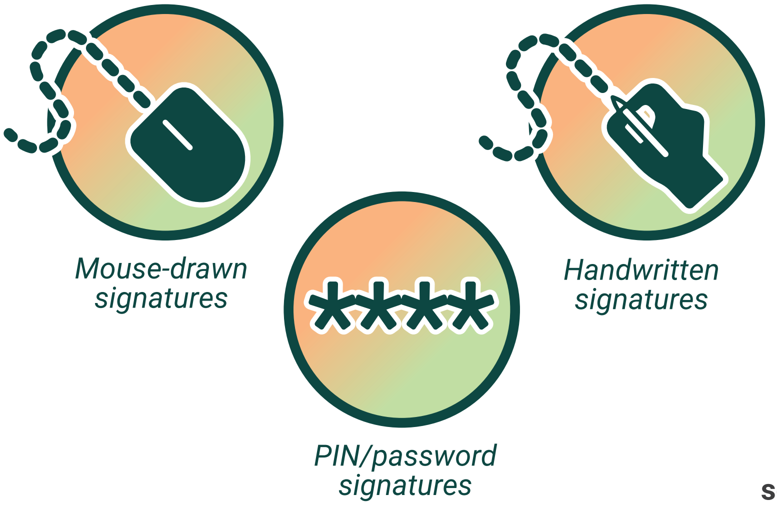
Under the sole control of the signer

Linked to a document in such a way as to prevent tampering

Capable of being authenticated

The Qualities of Legally-binding Electronic Signatures

Three Common Types of Signature Technology:



Mouse-drawn signatures

PIN/password signatures insert a single, fixed, signature image into each signed document when a user types a password or PIN.

Handwritten electronic signatures convert a user's signature accurately into pen events or a summary image.

Each method has different ramifications for security and authentication.

Why to Avoid Mouse-drawn Signatures

Signatures drawn with a mouse are generally not considered legally valid because they cannot be authenticated:

- They are not repeatable for the same signer,
- They are not captured accurately from a biometric perspective, and,
- There are no mouse-captured exemplars with which to make a comparison.

In addition, mouse data is available to any application running on the PC, and are therefore not secure.

Why to Avoid PIN/password Signatures

Companies invested in PIN/password signature stamps may claim that their technology is legally-compliant, but each of the inserted "signatures" is identical, as if they were made by a rubber stamp. Since any person could have typed the PIN, a forensic examiner cannot determine a signature's point of origin, falling short of the legal authentication requirements.

If a password is ever compromised, every document that person signed with the PIN method would be questionable, since it couldn't be proven which signatures were authentic.

For these reasons, businesses are advised, instead, to use electronic signature technology that creates a unique record for each signing instance.

Using Handwritten Electronic Signatures

Pen-and-tablet technology may seem a logical replacement for ink-on-paper signatures, but signature capture hardware manufacturers have their own specifications, data formats, and software methodologies that affect security, authentication, and legality.

Electronic Signature Security

For the sake of privacy and legal enforceability, an electronic signature must remain under the sole control of the signer to be valid under the national **ESIGN** electronic commerce law.

To satisfy this requirement, a signature must be:

- Placed or linked into the relevant document directly, with no interlopers or copies, and then,
- Bound to the document in such a way as to render document tampering detectable.

Without these critical features, it would not be possible to prove that a signatory did indeed assent to the agreement, or that the language in the document was unchanged after its signing.

In the paper-based universe, forensic examiners can test whether ink has been added or subtracted. With digital signatures, this is accomplished using a cryptographic hash and binding system, rendering a signature essentially “lost” if the contents of the agreement are changed.

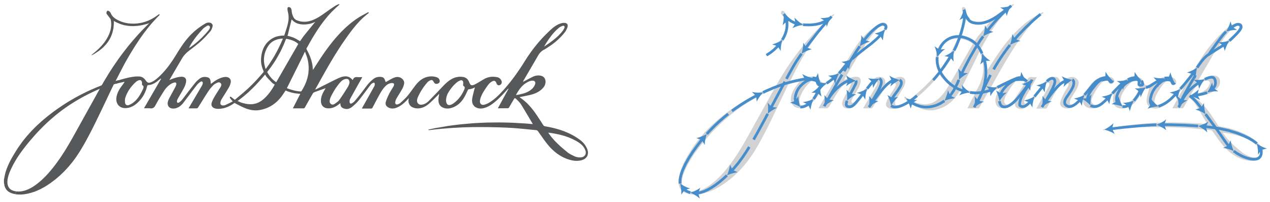
Signature Authentication

The most important characteristic of ink-on-paper signatures is that they can be analyzed by forensic experts, and compared to previous known samples for authentication. If a signature cannot be attributed to the signer, it is worthless. Electronic signatures are no exception to this, and a robust esignature solution will have authentication tools.

Systems that embed a signature image into an electronic document like a “rubber-stamp” (via PIN or biometric input) have less legal weight than faxed or photocopied signatures. The signature object is superficial with no biometric performance data, and unlike a fax transaction, there is no 3rd-party record of the transmission.

Several software providers offer automated template-based authentication. Each user must provide a number of signatures to create a template. This is unwieldy experience for one-time interactions, such as in a bank, pharmacy, or mortgage lender’s office.

Additionally, template-based authentication is often not a viable option because its signature data is not forensically significant.



Raw Pen Events: As the signature is drawn, the motion vectors are sampled and stored.

Raw Pen Events

The most accurate, reliable, and secure method of capturing a signature is in the form of Raw Pen Events. A file of this type contains no images or analysis, just the pen events and position converted at high speed. It can be stored in a database or bound to the contents of a document very securely since it does not exist as a common image file format. It cannot be easily copied, or viewed and used as a reference for forgers, since there is no embedded image.

Furthermore, since all original captured pen events are present in the esignature itself, a forensic expert can later examine it point-by-point using specialized signature analysis software.

Understanding Biometrics

While handwritten, digitized signatures may capture biometric data, all biometric data is not the same.

There is value in analyzing the data received from a signature pad, such as the point sampling rate, and detection of unusual time-related activity in signing. Slow-signing may indicate an attempt to trace or forge a signature.

Pen Pressure Measurement, however, is an unreliable biometric because it varies based on environmental factors (e.g. height of the signer, orientation of the sensor, etc.) from one signature to another. As a result, attempting to validate a pressure-oriented primary biometric is susceptible to unnaturally high false-negative responses.

The drastic variance between signatures makes even valid ones difficult to authenticate, so it is important that a signature capture technology has a means for authentication in the event of a legal challenge.

Conclusions

In general, when deciding which electronic signature system best suits the needs of your business, use traditional paper-based practices as a gold standard. If a specific technology mimics or matches these practices closely, it is probably a safe and reliable choice. The more technical shortcuts a system employs, such as creating multiple signatures with one stroke of a pen or keypad, or saving flat images in place of real, forensic-quality signatures, the more likely the system is to encounter difficulties and fraud in practice. With old ink-on-paper characteristics as your guide, your electronic document solution should be a signature success.

Getting Started

There's a lot of decisions that need to be made when choosing a signature capture technology for your business. Let the experts at Scriptel help you make the best choices.

Scriptel®
CORPORATION

Our Website:
https://scriptel.com
https://scriptel.com/shop

More Information:
info@scriptel.com
(877) 848-6824