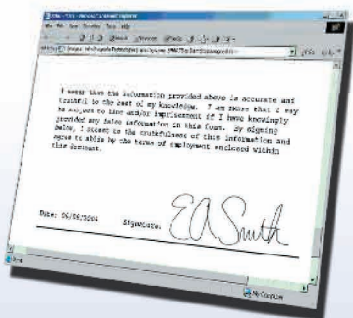


Electronic Signature Systems – A Guide for IT Personnel

Understanding Technology, Methods, and Authentication



As businesses continue to replace paper documents, contracts, and forms with more efficient and cost-effective electronic substitutes, electronic signature technology becomes an increasingly important investment. The cost and time savings of doing business electronically are evident across many sectors and industries, yet many companies are still choosing which technology or method is best suited to their needs. Creating, signing, transmitting, and storing any and all documents electronically and in such a way as to be legally-binding can seem like a daunting task, especially for small to medium-sized businesses. This article seeks to shed some light on the electronic signature solutions available and how to choose a technology that is best able to provide your business with the cost and time savings you're seeking.

What is an electronic signature, and how can I be sure my system is legally-binding?

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. Passed by the US Congress in 1999 and 2000, respectively, these two laws serve as the framework for electronic commerce implementation in the United States, as most state-level E-commerce laws are identical to UETA or a slightly altered version. These laws specify exactly what constitutes a valid electronic signature, as well as the conditions under which it is legally binding.

An electronic signature is a “sound, symbol, or process, logically associated with a document” such that it is:

- 1) unique to each user
- 2) under the sole control of the signer
- 3) linked to a document in such a way as to prevent tampering, and
- 4) capable of being authenticated

Several different methods and technologies exist for attaching “electronic signatures” to documents according to these stipulations. Two common types of signature technology that are widely available yet differ greatly in substance are PIN/Password signature stamps and digitized handwritten signatures. A PIN/Password stamp inserts a single fixed signature image into each signed document when a user types a password or PIN. Digitized handwritten signatures are captured with special pen-and-tablet systems that convert a user's signature accurately into pen events or a summary image. These methods have different ramifications for security and authentication.

An electronic signature must be unique to each signer, under their sole control, capable of authentication, and linked to the document to prevent tampering.

Signatures created by typing a PIN or password are identical in each document, making fraud detection difficult.

Why to avoid PIN/Password Signatures

While companies that provide PIN signature stamps may claim that their technology is legally-compliant because it qualifies as an “electronic sound, symbol, or process,” it falls far short of the holistic requirements enumerated above. As a practical point, each and every one of these “signatures” is identical in form and composition, as if they were made with a single rubber stamp. The appearance of the signature on a document is not a record of a person’s signature, but rather a result of a particular password being typed. A forensic examiner that views the signature image cannot determine its point of origin since any person could have typed the PIN or password. As such, PIN signature stamps fall short of the authentication requirements of criterion (4) listed above. Should a password become compromised, each and every document a person had ever signed with the PIN method would be questionable, since each signature appears identical and it cannot be proven which are authentic and which are fraudulent. For these reasons, businesses are advised to invest in an electronic signature technology that creates a unique electronic record for each signing instance, and not to rely on a “rubber stamp” technology. PKI digital signatures and certificates are simply a more complex version of “rubber stamp” technology, except that a larger (often 128-bit) encryption number is used, meaning it is too large to be remembered and typed. Portability is also limited because the key is permanently linked to a host computer, or a “secure” smart card which can be lost, stolen, or hacked.

Using Handwritten Electronic Signatures

A better choice for electronic commerce, especially with interactions involving the general public, are handwritten signature devices and software. While the use of any pen-and-tablet signature technology may seem to be the logical replacement for traditional “wet” ink-on-paper signatures, there are several issues to consider when choosing a system for your business. Signature capture hardware manufacturers have their own specifications, data formats, and software methodologies that affect security, authentication, and legality.

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 E-SIGN 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 terms of the written agreement, or that the language in the document was identical in form to the state in which it was initially signed.

There is no substitute for an effective security policy which prevents viruses, worms and data sniffers from residing on a client or server computer. Encryption gimmicks in a signature pad connected to a PC provide a false sense

of security if a rogue program or keyboard, printer, screen, memory, or usb data sniffer is also on the PC. Matters can be made worse if overly powerful and un-necessary processors and operating systems are employed in electronic signature devices, due to latent bugs and viruses or internal data storage and encryption; as these techniques further jeopardize and remove security monitoring and update capability from the hands of IT personnel.

On the other hand, there is value in monitoring and evaluating the integrity of data received from a signature pad, such as the point sampling rate, and detection of unusual time-related activity in signing which may indicate an attempt to trace or forge a signature (slow-signing effect). This capability is described further in US Patent 6,307,955.

Document security and signature binding are also important. If the signature is not linked to the contents of the written agreement, it has no real value since there would be no evidence of tampering or changes made to the terms post-signing. In the paper-based universe, forensic examiners can perform a series of sophisticated test using infrared, ultraviolet, and microscopic inspection to determine whether ink has been added or subtracted. In the electronic realm, 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

An important characteristic of ink-on-paper signatures is that they can be individually studied and analyzed by forensic handwriting experts, then compared to other existing samples for authentication. Perhaps the most significant challenge to the validity of an electronic signature is the issue of authentication, since few technology providers support their technology with verification tools. If a signature cannot be attributed to the purported signatory, it is worthless. Electronic signatures are no exception to this, and must be capable of authentication to be valid and binding. Insist that a technology provider have authentication tools and training in-place before selecting their solution.

Systems that embed a signature image into an electronic document (whether via PIN or biometric input) have less legal weight than faxed or photocopied signatures. Like “rubber-stamp” signatures, the object representing the signature is a superficial representation with no data linking the image to a biometric performance, and unlike a fax transaction, there is no 3rd-party record of the transmission. A bitmap, tif, or jpg image is not useful to a forensic examiner as it provides no detailed characteristics for analysis as is provided with original pen data.

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 of the signature, just the pen events and position converted at high speed. This data has the additional advantage of being stored in a database or bound to

There is no substitute for effective computer security. Encryption gimmicks in a signature pad connected to a PC provide only a false sense of security if a rogue program or keyboard, printer, screen, memory, or usb data sniffer is also on the PC.

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 e-signature itself, a forensic expert can later examine it point-by-point using specialized signature analysis software, if available.

Understanding Biometrics and Authentication

Another issue to consider with handwritten digitized signatures is the type of biometric data, if any, which is captured and stored in the signature file. Beware of pen pressure measurement. Pressure is an unreliable biometric measurement because of the high degree of uncertainty inherent from one signing instance to another. The level of pressure a signature pad senses for a single person will vary widely based on height and orientation of the signatory to the sensor, the person's mood, time of day, angle of the pad, size of the pen or stylus, calibration of the software, sensor age and wear, etc. As a result, a pressure-oriented primary biometric is susceptible to unnaturally high false-negative responses when automated or independent validation is attempted. In other words, when pressure is used to determine the validity of one or more signatures, it is far more likely to be a cause for rejection than for authentication, even if the signatures were created by the same user. Drastic variance makes signatures difficult to authenticate, even if they are valid.

Be sure that the technology provider offers software for signature authentication or signed records will not have an enforcement mechanism should legal challenge arise. Several software providers offer automated template-based validation, but this technique is often not a viable option for post-signature back-end authentication. Examiners cannot independently verify the signature. It also requires each user to offer enough signatures to create a sample template, which is unwieldy, especially in a one-time customer interaction in a bank, pharmacy, or mortgage lender's office. While automated validation software has many useful applications, be sure to choose a technology which is supported by independent forensic authentication tools. Many technology providers promise true biometric signatures, but lack the authentication tools to make their signature data forensically significant.

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. ■

Signatures saved as images are less secure and harder to authenticate than signatures saved as original raw pen data.