A GUIDE TO BEST AND WORST PRACTICES FOR ELECTRONIC NOTARY JOURNALS

Key Features and Benefits of Electronic Notarization Technology

The implementation of electronic signatures is saving businesses millions of dollars each year in transaction, processing and storage costs, and improving customer service in the process. Electronic notarization is a business process that also streamlines and speeds the notarization of both paper and electronic documents. This notarization process, being a key legal requirement of many high-value business and consumer transactions, requires the best that today's technology has to offer. A lack of effective electronic notarization technology will limit the benefits and savings of electronic signing, transmission, and storage of these documents. Conversely, the adoption of inadequate electronic notary technology will jeopardize the integrity of the entire process.

Electronic Notarization – A Guide for IT Personnel

Like the traditional paper-based process, electronic notarization must meet a set of technical requirements to be considered valid and binding. In addition to meeting the same practical function of a notary journal, an electronic system must overcome additional technical considerations before it can be reliably and safely used in a business environment. This guide will outline a set of best and worst practices for implementing electronic notarization across a business's process spectrum, using the existing paper method as the benchmark for functionality and security.

Best Practices for Secure, Reliable Electronic Notary Journal

Numbered, Sequential, Records

A notary's journal is a series of numbered, sequential records of each act a notary performs during the course of their term. In addition to the recorded dates for each numbered entry, the sequential order of their entry serves as an additional measure of integrity since a new entry cannot be "slipped in" between two previous ones. Also, the binding of a notary book works to ensure that pages cannot be inserted or removed without evidence of the tampering. These standard features of notary technology must carry over into the electronic realm for an E-notarization system to be valid and accepted for use in a given jurisdiction. If electronic records can be simply added-in or removed/deleted at will, then the integrity of the system is compromised, so are the records themselves. When choosing an E-Notary system, make sure that each entry is numbered according to the time if its entry and that entries or pages cannot be inserted or deleted. South Dakota and Oregon have already rejected one early attempt at an electronic notary journal product due to just one of many potential pitfalls in the technology.

Robust Electronic Handwritten Signatures, Encryption, and Verification

Like with a paper notary journal, the signatures attached to an electronic notary record should be capable of independent verification by forensic examiners and encrypted to the notary record in such a way that they are invalidated if any of the data is changed. Each signature should be encrypted to the record's contents, such as names, dates, ID types, and document copy using a hashing algorithm. As an additional privacy concern, signatures should be saved as raw pen events, free from any bitmap or jpeg images that could be stolen

and used to commit fraud. Beware of signature products that claim to capture and store biometric information, but do not have the software, tools, intellectual property, and training in place so that a forensic document examiner can render an opinion. One company that provides software, IP, and training for forensic document examiners is Topaz Systems, Inc.

Open-source Software tools, hardware options

Since notary regulations can vary widely between jurisdictions, an electronic notary system should be scaleable and customizable enough to meet the demands of differing jurisdictions. For example, California requires a fingerprint on some types of notarized documents, where Oregon might view fingerprint collection as in invasion of privacy. A notary system that requires a fingerprint will not satisfy users in both states, and a system that does not may cause some California records to be incomplete. Therefore, the technology should allow the responsible party to custom-tailor the notary application as required to be optimal in each jurisdiction. The software should also not lock users into a single supported option that may not meet their unique needs. For example, users in a state where fingerprints are not required should not be forced to buy a signature capture tablet with a fingerprint sensor attached.

Secure Non-Wintab Hardware Interface

For security, it is of critical importance that the electronic signature capture pad communicates with software through a secure interface. Graphic art-tablet interfaces, (i.e., Wintab) expose a signature by design to unauthorized capture by a rogue program. Therefore, the capture interface should support only one application connection to ensure adequate security. Under most electronic commerce laws, an e-signature is only valid if it is, among other things, under the sole control of the signer. Signature pads that use a Wintab driver to capture signatures do not satisfy this requirement, since this interface allows a device to be used by multiple programs at one time. In this case, the user's signature can be captured into other electronic documents or databases without their knowledge or consent. Therefore, ensure that signature capture hardware uses a single-point of connection direct interface to the signature tablet or pen.

Worst Practices - Things to avoid

Some of the so-called "worst practices" listed below are simply antitheses of the best practices listed above, but are stated as an explicit reminder of what not to do when creating an e-notary solution.

Saving Signatures as Images

This is a bad practice because an image can be easily copied, pasted, and viewed, and contains no useful biometric data for signature validation. It bears very similar characteristics to signatures that have been transmitted via a fax machine, which flattens the image and reproduced it without any of the nuances such as pen speed or stroke order that serve as evidence for authentication. Simply stated, an image of a signature is not a valid electronic signature. For display purposes, images can be generated at will from saved raw signature data, but not vice versa. Once a signature is flattened to an image and saved, the original pen events are lost.

Signature not encrypted to Notarization Date

If the signature is not encrypted to the notarization date using a hash algorithm or similar method, this date can be changed fraudulently without any means of detection. Ensure that your system binds signatures to the holistic contents of the notary record, including the date, or tampering will be undetectable.

Relying on Database Encryption/Password as Sole Protection of Record Privacy

A notary journal is normally kept in a locked safe or vault when not in use, where it is secure from unauthorized access. The same should be true of an electronic journal. Simply encrypting a database or using password input for access does not provide enough protection for the enclosed records. Consider systems that also require a notary's biometric input, such as fingerprint or valid signature, before the database is open for access.

No Independent Signature Validation Capability

Many signature capture systems offer automated template-based tools for assessing the authenticity of a user's signature. However, this template-based automated validation is not useful when independent authentication of a signature is required as proof of its validity in a legal setting. Requiring users to create signature templates when signing a notarized document may also constitute a violation of their privacy, especially if the security of the templates is compromised. As a result, consider using only signature pads and software that are supported tools which allow expert human examination of an electronic signature independent of a template.

Reviewing Best and Worst Practices for Electronic Notary Journals

Best

Numbered, sequential records
Handwritten electronic signatures encrypted, with independent validation capability
Open-source software supporting multiple hardware options
Secure, single-point of connection, non-Wintab interface

Worst

Saving signatures as images
Not encrypting signatures to notarization date, and all other data
Password/Encryption as sole database security
No independent (non template-based) signature validation tools, IP, and training.

About the Author:

Paul Michael Zank is Marketing Manager for Topaz Systems, Inc. As such, one of his tasks is to find ways to simplify and explain electronic signature requirements and practice for use by thousands of companies worldwide. He also coordinates forensic document examiner training for electronic signatures, strategic partnerships, and is co-author of a pending patent in the field of eSign authentication. He holds BA degrees in Media and Political Science from the University of California, San Diego.