Speech in Electronic Signatures

Voice biometrics can play a role, but we'll still need notaries

Even though they're likely to be total strangers, notaries public attend some of the most momentous events in our lives. From real-estate transactions to wills and trusts to international adoptions, when it comes time to complete an agreement, a notary public will be present. He could even be one of the best lines of defense we have against identity theft.

The more than 4.5 million notaries in the United States are legally empowered to identify the parties to a transaction and certify the validity of a document. But the notary's most important tasks are certifying that the signer was competent to sign the document and that the signer did so willingly.

Richard Hansberger, director of eNotarization at the National Notaries Association (NNA), states that more than 900 million transactions are notarized in the United States annually. Increasing numbers of transactions that were traditionally effectuated on paper are now being created, processed, and completed digitally, entirely without paper.

> **One of the biggest problems is that digital signatures have the potential for misuse.**

To accommodate the transition into the digital arena, the NNA created an electronic notary seal (ENS). The software used to affix the ENS currently requires users to log in with fingerprint biometrics, but Hansberger believes that voice biometrics is a logical next step, envisioning voice as a secure and more natural way for the notary to log into the ENS software. Voice biometrics could also be used if a notary's ENS becomes compromised. The notary could call a designated telephone number and report the compromise, thereby revoking the certificate immediately, before unauthorized users could fraudulently notarize any records.

A Matter of Law

Because of the trend toward digital transactions, digital acknowledgements are becoming increasingly important, resulting in legislation on the state and federal levels. The federal Electronic Signatures in Global and National Commerce Act (E-Sign) and the Uniform Electronic Transactions Act (UETA), which have been adopted almost universally by state governments, accord electronic documents the same legal effect as paper documents.

In several states, including Minnesota, Nevada, and Utah, legislation was enacted stating that when a signer uses a verifiable digital signature, the need for the signer to personally appear before a notary is obviated. This wording authorized unlimited and unwitnessed use of a digital certificate while eliminating the requirement of the physical presence of a notary public. Because of the inherent danger in this protocol, the legislation has been repealed in Utah and Minnesota. While the Nevada law is still in effect, Nevada does not allow any e-notarization because the state concedes its inability to regulate it.

One of the biggest problems is that digital signatures have the potential for misuse. The certificate could be issued to an imposter or accessed and exploited by an unauthorized person, or the certificate's owner could be coerced or manipulated into using the certificate to sign an electronic document unwillingly or against his interests.

Security features including biometrics, public-key interfaces, third-party time stamps, and hash algorithms can be integrated into the electronic document process to ensure a document is not altered or accessed inappropriately. Biometrics could even be used to validate the identity of a party and serve as a signature. But relationships that require notarized documentation of the agreement must be entered into willingly and by parties who are competent if that documentation is to be enforceable in court. None of the above-mentioned security solutions ensures the volition and competence of the signers.

Absence of the neutral third party certifying the parties' willingness and competence might make it easier for parties to attempt repudiation of the instrument. This makes the personal appearance before a notary fundamental because it is the only way to ensure the signer's identity, acknowledgement, volition, and awareness. "All of the challenges to e-docs involve documents that are not notarized," Hansberger points out.

The numbers of electronic signatures and associated digital transactions can be expected to increase. But, because many of these transactions are of high-value or sensitive natures, we need to ensure that the security of the parties is commensurate to the security associated with traditional paper documents. Biometrics may prove to be an integral part of the solution. With all of the technology-based safeguards available, including biometrics, none are as powerful a tool in maintaining the integrity of the process as human perception. Because of this, it is unlikely we will ever completely remove the human element. ☒

Robin Springer is the president of Computer Talk (www.comptalk.com), a consulting firm specializing in the design and implementation of speech recognition and other hands-free technology services. She can be reached at (888) 999-9161 or contactus@comptalk.com.