Bloomberg BNA Electronic Commerce & Law Report™

Source: Electronic Commerce & Law Report: News Archive > 2015 > Latest Developments > News > Contracts: Company Needs Dictate Which E-Signature Solution to Use

Contracts

Company Needs Dictate Which E-Signature Solution to Use

By Alexis Kramer

Oct. 8 — Modern electronic contracting technologies are capable of capturing not only a digital image of a signature but also performing other important services for their users: authentication of the signer, a guarantee that the document has not been altered, logging as to time and place, along with a variety of other helpful features that assist in securing courtroom admissibility or regulatory compliance.

However, many parties engaging in electronic contracting need only a small subset of these services, if indeed any at all.

Electronic signature experts consulted by Bloomberg BNA advised parties considering electronic contracts to carefully weigh the costs of employing electronic signatures against the specific risks they must mitigate with respect to the transaction.

These experts said that companies in regulated industries (e.g., insurance, banking) would benefit most from public key encryption and other technologies that electronically seal a record, along with audit trails to capture every step of the signing process, to reduce the risk of authentication and repudiation claims. On the other hand, they said, the need for security and authentication techniques may be minimal in other types of transactions, where the value being exchanged or the opportunity to repudiate a signature is low.

Companies employ e-signature solutions — which can be anything from an encrypted digital signature to a simple password — as they digitize their businesses and eliminate the need for traditional paper contracts. According to a recent study by Forrester Research Inc., the number of transactions using e-signatures has increased by 53 percent in the past three years, with the number expected to increase from 210 million in 2014 to 700 million by 2017.

BNA Snapshot

Electronic Contracting

Key Development: Electronic signature experts advise companies who are most concerned about the risks associated with e-contracting to consider high-tech digital signature technology, whereas other companies should assess the costs and benefits and decide on an individual basis which type of e-signature solution is best for their business.

While the Uniform Electronic Transactions Act (UETA) — a model state law adopted by 47 states and the District of Columbia (9 ECLR 672, 8/4/04) — and the federal Electronic Signatures in Global and National Commerce (E-Sign) Act, 15 U.S.C. §7001 et sec. (6 ECLR 165, 2/14/01), give electronic signatures the same legal status as handwritten ones, they are technologically neutral regarding the type of e-signature required for a transaction.

The statutes define "electronic signature" as an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. Intent can be shown from the context of the record or the surrounding circumstances.

Mitigating the Risks

E-signature solutions include typed names, clickwrap signatures, recorded voices, biometric measurements (e.g., retina scan, fingerprint matching) and digital signatures with public key encryption. Margo Tank, a partner at Buckley Sandler LLP in Washington, told Bloomberg BNA that not every transaction needs the most advanced e-signature technology.

"It's not a one size fits all," she said, "as long as you have sufficient controls in place to address the risks at issue, such as authentication and record integrity."

Patrick Hatfield, a partner at Locke Lord LLP in Austin, Texas, shared a similar view. To determine which type of technology is best for each business, he recommended that practitioners identify and focus on the transactions with the highest volume for their companies or clients and determine how great each of the following six risks are:

- authentication (What is the risk that the electronic signature was forged?);
- repudiation (Could there be claims that "I never saw that document"?);
- regulatory compliance (Have the rules and regulations governing the transaction been met?);
- admissibility (Is the electronic record admissible into evidence?);
- adoption (Is the e-contracting process too cumbersome for a consumer to use?); and

• relativity (Are the risks of the e-contracting process greater than the risks of a traditional contracting process?).

Hatfield told Bloomberg BNA that companies looking to mitigate the authentication risk should use an e-signature solution with a "shared secret," or a combination of questions that only the real person is likely to know, such as a driver's license number, social security number or the security code on the back of the credit card. Companies that run a credit report can learn the answers to verify the signer.

Hatfield said that although biometric methods can be reliable for authentication, they are likely not feasible for most companies because they require the person to have been previously measured.

According to a recent report of the Standards and Procedures for Electronic Records and Signatures (SPeRS), an eCommerce initiative sponsored by the Electronic Financial Services Council, more secure signature methods may be desirable for transactions more likely to produce disputes over authenticity, such as insurance or credit transactions.

Regarding repudiation, the report found that this risk is increased if either the value being exchanged in the transaction or the exposure to liability for conducting the transaction is significant. According to the report, public key encryption and random number generators provide a very low risk of repudiation unless the generator or private encryption key was accessible to an unauthorized person. Biometric signatures also provide a relatively low opportunity for repudiation unless the biometric information was compromised.

Hatfield said that the repudiation risk can be reduced by technology that electronically seals a record once it is signed (e.g., public key infrastructure (PKI), "hashing" the record, digitally signing and encrypting the record), along with an audit log to record each significant step of the transaction.

Michael Laurie, co-founder of e-SignLive by Silanis, a widely-used e-signature provider, told Bloomberg BNA that with regard to repudiation claims, e-signature technologies providing layers of security and capturing the e-contracting process are significant from an enforceability perspective. "Being able to track the process is really important," he said. "It does an incredible job of keeping us out of court."

Approaches to Electronic Signatures

Typed name: or a digitized image of a handwritten signature.

PIN or password: for controlling access to the contract, as well as protection against modification.

Random number generator: a unique character string embedded into the contract.

Click-wrap signature: mouse-click an "OK" or "I agree" button to indicate assent.

Biometric measurement: a retina scan, fingerprint matching or voice recognition.

Public key encryption: a cryptographic system in which a pair of keys is used to encrypt and decrypt a message.

Shared secret: a combination of questions that only the real signer would know, e.g., driver's license number, social security number.

Tamper seal: an algorithm that can be used to detect if a record has been altered.

Audit trail: records and reproduces web pages, documents and disclosures displayed during each step of the signing process.

Complying with Regulations

To ensure compliance with government regulations, the report said companies should consider whether their transactions are covered by any specific laws that restrict signature options. For example, the U.S. Food & Drug Administration's electronic signature regulation, 21 C.F.R. Part 11, provides that e-signatures must be unique and verified, and that the person using an e-signature must certify to the FDA that it is intended to be the legally binding equivalent of a traditional handwritten signature.

Typed names and clickwrap signatures are likely not acceptable under the FDA's e-signature guidelines, the report found.

To ensure companies satisfy certain disclosure requirements in their transactions, for example, under the Securities Act of 1933 and other federal securities laws, Hatfield suggested using e-signature solutions with an audit log that tracks each form presented, completed and signed. The audit log technology can also be used to track the signing of a HIPAA Authorization form, he said, which patients are required to sign prior to a health care provider releasing that person's medical records.

Evidentiary Burden; Paper Process Compared

Some e-signature solutions, said Laurie, fail to show from an admissibility perspective who was present, how the process was followed or whether the document was modified after signing. "It's a fallback on the rules of evidence when you get to court," he said.

Laurie said that e-signature solutions built on digital signature technology should collect persuasive electronic evidence in the form of an "active audit trail" by recording and reproducing the exact process used to build the signer's understanding of what they were agreeing to. This evidence can include the exact appearance and order of every displayed web screen, document and legal disclosure, along with how long a person spent on each page and each action taken.

Tank, a co-reporter for the SPeRS drafting committee, said that while digital signatures are no more enforceable than the less sophisticated ones, the evidentiary burden in the event of a challenge may be easier if the signing process being challenged is not thoughtfully developed.

Digital signatures typically contain three attributes: a certification authority (independent verification of transaction parties), a method to express intent to be bound to a transaction if required and an encryption mechanism to enable record integrity. Tank said that many companies also use a tamper seal (a hash), which is an algorithm that can be used to detect if a record has been altered.

Hatfield added that having a person familiar with the company's process and technology available to testify under oath can help a company meet the admissibility standards required by the courts.

Hatfield also said companies should time each transaction to ensure it doesn't take too long to complete. If it takes longer for a consumer to complete an e-contract than a paper contract, he added, the company should switch back to paper.

On the whole, he said, a company's selected e-contracting process should be "no riskier than and more efficient than a paper one."

To contact the reporter on this story: Alexis Kramer in Washington at akramer@bna.com

To contact the editor responsible for this story: Thomas O'Toole at totoole@bna.com

---

ISSN 1523-5661