

Opinion

DIGITAL SIGNATURE LEGISLATION MUST KEEP PACE WITH TIMES

With the holidays behind us and Congress returning to a new agenda, analysts predict that some form of digital signature legislation will likely be passed this year. Those same analysts claim such legislation is critically important and long overdue. Symbolically, it shows that American business will continue to be a leader in the increasingly wired world economy. Without such legislation, they argue, the enormous potential of e-commerce will never be realized.

Clearly this legislation is critical to the success of e-commerce, as well as e-finance, however strong security technology must be in place in order for this legislation to work.

The proposed legislation relies in large part on the effectiveness of various forms of cryptography and, in particular, on the Public Key Infrastructure (PKI). PKI systems produce "digital certificates," which are used to bind names to cryptographic keys. These certificates are then used to form digital signatures on electronic records, attesting to both the content of the record and the identity of the signer. While digital signatures can identify the "who" and "what" aspects of a digital document, they cannot by themselves identify "when" a signature was formed. The ability to securely determine the time at which a digital record was signed requires an additional service, called a secure digital time-stamping service.

Secure digital time-stamping services can provide a number of enhancements to a basic PKI. As many professional organizations have recognized, the proper functioning of a PKI often includes the application of secure digital time-stamps in certain areas of operation. Truly effective data integrity systems must incorporate the best of these technologies in order to be effective.



Wes Doonan, Surety Technologies Inc.

Various features of digital time-stamping can improve the integrity of a PKI system. First, the PKI can provide additional non-repudiation services to users of digital certificates, by enabling those users to time-stamp their digital signatures. Time-stamping a digital signature is in some ways similar to visiting a notary public to certify a paper document. Second, the various internal operations of the PKI itself can be time-stamped, in order to provide information that can be audited when disputes arise.

Digital signatures on important documents, like mortgages and wills, need to be provably correct for long periods of time.

However, digital certificates have a finite lifetime, sometimes much shorter than the lifetime of the document itself. If the digital signature and certificate revocation data are time-stamped while the signing certificate is valid, it is possible to prove that the signature is valid even beyond of the lifetime of the signing certificate.

Or consider a scenario in which the signer of an important digital document later wishes to repudiate that signature. The signer can cast doubt on the validity of that signature by falsely reporting the compromise of his private key. Had the document, signature and certificate revocation data been digitally time-stamped at the time of signing, an attempt at repudiation through "false compromise" would be much more difficult.

As e-commerce continues to grow, truly effective digital signature legislation will need to keep pace with increasingly complex digital security issues. Likewise, digital security systems will need to adapt to the growing security needs of the new online citizenry.

*Wes Doonan is Director of Engineering for **Surety Technologies Inc.**, a Reston, Va.-based provider of secure time-stamping services for the internet. Surety can be found online at www.surety.com.*

MORTGAGEIT.COM ADDS NATIONAL BROKER NETWORK

Independent Brokers Inc., a Rhode Island real estate broker network, has become a member of **MortgageIT.com's** Real Estate Affiliate Program. MortgageIT will provide electronic commerce marketing resources to the IBI's member firms. The program allows real estate agents to pre-qualify homebuyers for loans.

Last month, New York-based MortgageIT signed an agreement to provide mortgage loans via the **Govworks Inc.** site. Govworks (www.govworks.com) is an information and services site connecting consumers to local government nationwide.