IDG.net
CIO WebBusiness
Five Surefire Strategies for Getting Fresh Page 24
Section Two • March 1, 1998

ETHICAL DILEMMAS AND LEGAL LANDMINES

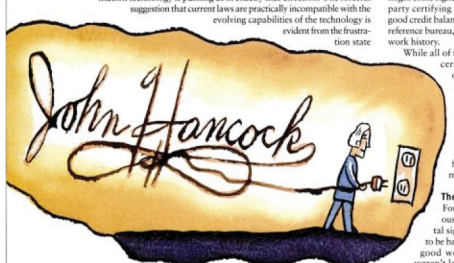
**GRAY MATTERS**

# In Code We Trust

*Lawmakers are struggling to dot the i's in digital signature legislation. Maybe they shouldn't bother.*

BY FRED HAPGOOD

ONE OF THE MORE DELICIOUS FANTASIES PERVADING TECHnical circles is that someday the Internet will allow society to dispense with laws and lawyers, at least in civil cases involving contracts and torts. The idea has plenty of skeptics, as it should, and yet sometimes it really does seem as though information technology is pushing us in exactly that direction. One forceful suggestion that current laws are practically incompatible with the evolving capabilities of the technology is evident from the frustration state governments have suffered trying to impose conventional legal thinking on the new authentication technology known as digital signatures.




Digital signatures are based on a class of codes that have two keys. What is encrypted by one key can be decrypted only by the other and vice versa. If Alicia keeps one key private while making the other public, then any text that can be decrypted with her public key could have been encrypted only with her private key and therefore only by her. Such texts are said to have been "signed" by Alicia. In some ways, such signatures represent a higher degree of authenticity than written signatures because they are harder to forge—although they can be stolen.

An especially attractive feature of digital signatures is their ability to allow a text to be signed by many people; a text can be encrypted once by a procurement officer, then mailed to his superior who will encrypt it again with her private key, and finally mailed again to the bank holding the company's credit line for a third pass. A vendor decrypting such a purchase order can be confident of the identity of the person making the order, that she had the authority to make the order and that the company has the credit to support the purchase. Similarly, a digitally signed response to an RFP might come signed with one key from a party certifying that the bidder had a good credit balance and another from a reference bureau, testifying to his or her work history.

While all of these functions could certainly be performed on paper or with EDI, digital signatures are cheaper, faster and more flexible. As important as the security applications of the technology might be, many feel its future as a management tool is even rosier.

### There Oughta Be a Law

For years it seemed obvious that to be useful digital signatures would have to be backed by the law. What good would they be if they weren't legal? What company would issue certificates if its executives didn't have a clear grasp of their liabilities in case they made a bad call? Who would accept certificates unless the issuing company was willing to accept some liability? And while the law is not always quick to address issues that are fundamentally technological, it did appear to respond quickly to this topic.

ILLUSTRATION BY ROBERT NEUBECKER





**GRAY MATTERS**

In 1991, the American Bar Association formed a committee to draft legislation on the subject, and by 1995 one state, Utah, passed legislation based on the committee's work. In essence, the deal was this: Companies wishing to use digital signatures to certify facts about others (such as identity, credit rating and reputation) could limit their liability in return for paying a $500 fee to an appropriate state agency, posting a $75,000 bond and conforming to a fairly detailed set of regulations controlling procedures for handling certificates. (Details at *www.commerce.state.ut.us/web/commerce/digsig/dsmain.htm.*) But no sooner had the legislation passed, than enthusiasm for it began to cool. First, the fee structure seemed incompatible with the global ambitions of the technology. Were companies that hoped to use digital signatures expected to pay fees and post bonds in every jurisdiction on earth? As of this writing, two years later, exactly one company has signed up.

Last May, the California legislature passed a more restrained law that required no fees and established no new state agency. It simply described a set of criteria that would allow a company to appear on an approved listing of authorities who were certified under that state's laws. One business implication of the law was its presumption that if and when the state started using digital signatures, its agencies would feel compelled to do their procurement though companies on that list.

This was an improvement over the Utah legislation—backers viewed it as more technology-neutral—and, as of this writing, 10 states have followed California's lead. However, even that law has spurred objections, specifically over the thorny problem of detail. To a lawyer, detail is a good thing; it makes clear when suits can be filed and when they can't. However, detail in a law governing such a new technology, especially one fated to penetrate so many jurisdictions in such short time, was more problematical than most.

For instance, the Utah law prohibited companies from giving operational responsibilities to any employee convicted of a crime involving deception within the past 15 years. Suppose some other state or nation imposed a different limit, or defined "operational responsibility" or "deception" in other ways? How were those differences to be handled? Would each certificate have to reflect the laws pertaining to the specific jurisdictions involved, or should they be made generic, and if so, by whom and how?

The same problem arises with the California criteria. For example, a company on the list will be dropped unless it submits proof of continued compliance every two years. But obviously there's nothing magic about a two-year time frame. Such differences would, of course, arise in an unregulated sector, but in the private sphere variations could be ironed out in a conference call or, at most, by putting together a standards committee. Only legislatures could change statutes, and the glacial pace of legislative action would seem to guarantee long periods of confusion and conflict.

> **"Perhaps too much emphasis has been given to the role of government as lawmaker."**
>
> *–Daniel Greenwood, Massachusetts deputy general counsel*

### Make No Law

As these considerations have simmered, they have engendered something resembling a race to the regulatory basement, with various states competing for the honor of ruling with the lightest hand. The winner so far seems to be Massachusetts, which has proposed a draft law that did nothing but rewrite statutes to make sure that parties were free to use digital signatures if they wanted to.

"Some laws required writings on paper and signatures in ink," says Daniel J. Greenwood, a Massachusetts deputy general counsel working in the IT division of state government. Greenwood thinks that once digital signatures have been made not illegal—as opposed to being made legal—governments should wait before assuming further roles in regulating electronic commerce. "Important though it may be, perhaps too much emphasis has been given to the role of government as lawmaker," he says. Digital signatures inaugurate a new trust infrastructure in world commerce: Formal, explicit exchanges of authority and authentication will characterize more relationships and change more rapidly than in the era of paper contracts. Managing this transition even within a single company is complicated enough, requiring close continuous consultation among corporate counsel, core management and CIOs.

Greenwood's view is that until we know about how these new reputation economies will work, legislation on any level would end up doing more harm than good. His argument seems to draw strong support. He adds that, on the basis of his experience in state government, many organizations would benefit from running an "authentication audit" that carefully examined who has to approve what, when. One of the side benefits of moving to digital signatures is that this audit occurs automatically as a necessary part of the transition.

For the moment, digital signatures exist in a benign legal limbo. Their usual application is in cheap browser-server authentications (as in SSL). Vendors accept no liability whatever for these exchanges, but the technology seems useful enough anyway. Beyond this is a range of experiments within networks of established business relationships, often using intranets or extranets. These are controlled by negotiations worked out on a case-by-case basis, by preexisting contractual relationships or by regulations governing the overall business mission, such as the rules defining credit card liability.

In time, the role of the state will likely clarify itself and more appropriate laws will be based on that enlightenment. Or perhaps all the players will find life in this libertarian limbo pleasant enough for a protracted stay. CIO

*Fred Hapgood is a Boston-based freelance writer. He can be reached at* hapgood@pobox.com.