

by Jonathan Rosenoer

GETTING TO DIGITAL SIGNATURES AND ELECTRONIC COMMERCE

Aux États-Unis, aucun système de cryptage n'a pu, jusqu'à présent, rallier l'assentiment des autorités publiques et de l'industrie à la fois. On croit souvent, mais à tort, que c'est à cette absence de consensus qu'il faut attribuer le retard du développement du commerce électronique. Pour prospérer sur l'Internet, les entreprises ont besoin d'une « signature » numérique puissante bien plus que d'un système à toute épreuve de protection de la confidentialité.

It is widely accepted that the US government has been unable to forge a national consensus around an encryption policy acceptable to law enforcement (including intelligence agencies) and industry. This failure is holding up the development of electronic commerce. Businesses are uncomfortable working in an environment where they cannot be sure of the identity of the other party and that an agreement they make can be enforced. Although the key to removing this certainty is strong public-key cryptography, resolution of the commerce issue does not depend on prior determination of a national encryption policy. To succeed and generate online revenues, businesses need strong digital signatures more than bulletproof confidentiality.

For many years, the public has worked with communication tools that transport information effectively, but do not offer high degrees of privacy or confidentiality. Postcards, for example, are not a good medium for sending private messages. The limitations of early cordless telephones were not hard to discern, particularly when you could hear your neighbours' cordless calls piped through your own cordless handset. The public generally adjusted its behaviour in recognition of the risks involved. Where the risks have not been well understood, law enforcement has been able to exploit the opportunity. US courts allowed law enforcement unrestrained eavesdropping where the circumstances showed the parties involved had no reasonable expectation of privacy. Courts have also allowed communication surveillance in cases where the cause shown was sufficient to meet constitutional protections regarding searches, seizures and privacy.

Recently, three technologies arrived in the marketplace — e-mail, the Internet and public-key encryption — together promising widespread, secure, public communication. Law enforcement has reacted with alarm at the prospective loss of access to private communications and lobbied against relaxation of controls on the use of strong encryption. The government has also introduced systems and schemes, such as “key recovery,” that would guarantee access to the unencrypted (plain) text of communications.

These efforts have been met by a range of opponents, including computer software companies, the computer security industry and civil libertarians. Critics of encryption controls and regulation blame the government for retarding the growth of electronic commerce and for driving the development of an overseas encryption and security industry.

The debate between the parties is polarized and highly vocal. Unfortunately, it seems unlikely that an acceptable US cryptography policy will emerge in the near term. By framing the debate in terms of a feared inability to detect and prosecute drug dealers, terrorists and child pornographers, the government has made it very difficult for anybody to present a contrary view without running the risk of being viewed as naive and “unpatriotic.” This remains the case despite indications that encryption is not obstructing a large number of investigations, and, to the contrary, that communication weaknesses is enabling crime — accounting for the largest portion of economic and industrial information lost by US corporations, to the benefit of foreign governments and corporate intelligence collectors, as well as others.

The problem is exacerbated by the government's repeated calls for “key-recovery” systems. Technologists seem to agree that the key recovery focus is not sustainable, if for no other reason than deployment of such systems is beyond the experience and current competency in the field. They also point out that there is no viable economic model to account for the cost of key recovery systems.

Washington insiders recognize substantive problems with the government's stance. But there has been no significant change in the government's position, even in the face of bipartisan, concerted and significant opposition by industry, supported by demonstrated, resulting economic loss.

If national consensus cannot be achieved on the global issue of strong encryption, it is important to recognize the fact and concentrate on areas where agreement can be reached. And for electronic commerce to succeed, there is one required element that depends upon strong cryptography, but not necessarily confidentiality: the digital signature.

Without digital signatures, companies are hard pressed to engage in electronic commerce. Businesses require assurance that an electronically signed document can be enforced against the sender. At present, there is no definitive court decision ruling that an electronic document can be "signed" electronically in legal systems and in circumstances where the signature remains as a formal requirement of law.

This "signature" issue is intimately related to a technical, legal issue of proof. In a court case, a party seeking to enforce a contract has the burden of proving that (1) the document was signed by the person who it purports to have come from, and (2) that the document presented is, in fact, the one that was signed. In the context of electronic communications, the burden can be carried if the parties used strong public-key algorithms (1024 bit key sizes or better), providing user authentication and data integrity checks.

Widespread acceptance and availability of standardized, digital signature and identification software would resolve the repudiation issue. Such software could be strong enough to assure that documents signed in one year would be secure for many years to come. Courts and businesses would have a known and stable platform on which to base their respective legal and business decisions.

The US Secretary of Commerce has blamed both industry and law enforcement for the failure to find a reasonable compromise between the need to monitor criminal activity and the need to offer consumers strong security for on-line transactions. As the national interest supports reaching a compromise, the government should actively encourage the development of an acceptable, international digital signature and identification standard by a trusted implementer.

Jonathan Rosenoer is Managing Director — Strategic Alliances, Arthur Andersen Knowledge Enterprises, San Francisco, California.

by Jim Carroll

ELECTRONIC COMMERCE AND THE PAPERLESS ECONOMY

L'Internet sera l'épine dorsale de l'économie du XXI^e siècle. Il reliera l'ensemble des systèmes informatiques et des puces d'ordinateurs à travers le monde. Or, le commerce électronique est une extension logique et inéluctable du rôle des ordinateurs au sein de l'économie, les transactions sur papier cédant graduellement le pas aux transactions électroniques.

It is one of those phrases that seems to have suddenly appeared on the scene, and which is used in almost reverent tones by the "digerati." The truly trendy use the phrase "e-commerce," while IBM has gone so far as to customize it to the more palatable word "e-business."

Even given the sudden prominence of the concept, I find that many executives seem to be either mystified or skeptical of the concept of e-commerce. For many, it is yet another complex invention by the so-called "gods" of the computer revolution, one that is worthy of the disdain of those who have been burned by so many ill-fated computer promises of the past. For others, the unrelenting hype that surrounds the concept means that it is simply another tantalizing opportunity that will go the way of so many magical promises of the past. There is little appreciation among the executive crowd, even given the incessant focus on the topic Internet, as to what electronic commerce is really all about.

To me, the whole concept of e-commerce is quite simple — it is merely but the second phase of mankind's relationship with computer technology. The first phase,