ALTERNATIVE VISIONS FOR LEGAL SIGNATURES AND EVIDENCE

Summary of Remarks at Financial Cryptography '97
Anguilla, BWI, February 27, 1997

By Benjamin Wright

I have two messages: (a) there is more than one way legally to sign an electronic transaction; and (b) the environment in which a transaction is effected and recorded can affect your ability to prove it to a judge and jury, perhaps more than could the strength of the cryptography used.

It is popular to believe that public key digital signatures are the only good way to sign electronic business messages for legal purposes. This belief has given rise to digital signature legislation in the state of Utah, which has been followed by the state of Washington. (For a comparison of the Utah law with other electronic commerce legislation, see <http://www.state.ma.us/itd/legal>). Part of the argument made for this legislation is that in an "open system like the public Internet" a digital signature is the only effective way to establish proof that an identified person approved a message.

I agree that digital signature is a superbly useful technology. But I'm skeptical of the Utah legislation and the rationale behind it.

The Utah Digital Signature Act invests a lot of power in the private half of a key pair. The private key can be used to sign an unlimited range of transactions -- from commercial contracts, to wills, to divorce agreements. Then it gives the holder of such a key abundant incentive to protect it and not lose control of it. The Act says that, after a proper X.509-style certificate has been issued, the owner of a private key has an affirmative duty not lose the key. Moreover, says the Act, it shall be presumed in court that any document signed with the private key is the legal responsibility of the key owner.

This formula concentrates lots of reward and risk onto the private key. The formula helps recipients of signed documents feel quite comfortable about who is legally responsible for the documents. This may be desirable if the recipient is relying on an electronic cash note issued and signed by a bank. But on the other hand, the formula places a tremendous demand on the key owner. The consequences to the owner of being negligent could be devastating. Let the key fall into the wrong hands, and the owner could find herself bound to an unexpected bill of sale on her house or an unintended child custody agreement with her ex-spouse.

One conceivable way to ameliorate the Utah Act's extreme consequences would be for key owners, at the time their public keys are certified, to adopt disclaimers of certain liabilities. For instance the certificate associated with the owner's key pair could state that it is only effective with respect to a limited range of transactions (e.g., only sales of crude oil), and not to other transactions. This idea has merit, but no one has tried it so far, and it faces two challenges.

First, the Utah Act is not written explicitly for this idea. Of course, one might be able to shoehorn it into the interpretation of the present Act, or one might persuade the legislature to incorporate it into the Act by future amendment. Second, disclaimers and limits of liability have to be worded and interpreted very carefully, lest they cause confusion. Carefully worded disclaimers may turn out to be more than just a sentence or two in length. Signing with digital signatures might therefore be made more difficult (might be burdened with more redtape) because each verification of a signature would require careful exegesis by a lawyer of the disclaimers in the relevant certificate.

Biometric Example

In my presentation I demonstrated an alternative to the Utah vision for digital signatures. The purpose was not to set up the alternative as an all-purpose replacement for digital signature, but rather to illustrate a different way to think signatures and evidence. I demonstrated a technology called PenOp <http://www.penop.com>, which allows an individual to sign an electronic document using his handwritten autograph. The individual grasps a stylus and writes his

name on a digital tablet attached to a computer. He sees on the computer screen the image of his autograph associated with the document he is signing.

In effect, by signing he performs a cultural ritual that makes clear to him he's becoming legally bound to the document -- such as a bank loan agreement, an insurance contract or (heaven forbid in Anguilla!) an income tax return. He need not be educated about the meaning of the event or the importance of protecting keys, passwords or the like.

PenOp captures an image of the signer's autograph. It also measures the rhythm of his pen strokes as he signs -- in effect a type of biometric measurement. The software encrypts the image plus measurements to a hash of the signed document, thus creating a record showing what the signature data are attached to and whether it ever changes after the data are attached.

The result of the PenOp process is modest evidence as to the document's origin -- evidence similar to that typically captured with a paper-and-ink document. In the event of a dispute, a questioned document examiner (handwriting expert) could compare the image and measurements captured by PenOp with specimen signature measurements obtained at a different time. To get a good reading on proof of document authenticity, the document examiner would also need to consider all of the other facts and circumstances of the case -- the full relationship between the parties, the testimony of witnesses, the exchange of money, goods or other documents and anything else that might be relevant.

Proof of authenticity would not rely heavily on any single thing. Whereas under the Utah vision, proof depends greatly on the control of a single key, the proof under a biometric approach (represented by PenOp) must look at all the relevant evidence, with no predefined rules on which evidence is superior. The signature image and biometric measurements might be useful and relevant evidence, but not necessarily dominant evidence.

Controlled Environments

This approach to proof and records, which is applicable to authentication technologies other than just PenOp, elevates the importance of the security of the electronic environment in which commerce occurs. Controlled (or "closed") environments, even those existing on the Internet, can provide relative degrees of security that contribute to the believability of evidence and records (biometric, cryptographic or otherwise). The transaction of business within the context of an encrypted extranet or virtual private network, for example, can help to show that records of that business are credible.

Credibility is enhanced to the extent the security of an environment is competently cultivated. If the operator (or webmaster) can show that he maintains a respected standard of care, protecting records from abuse and keeping miscreants out, then judges and juries are more likely to believe his records showing that a particular person signed or approved a particular transaction. Methods for achieving control can certainly include cryptographic procedures, but they must include much more -- such as closing off backdoors to a commercial web site. (For ideas on operator standard of care, <http://www.ncsa.com/webcert/webcert.html>). In this context, crypto is viewed as a tool interdependent with other tools. Crypto, while important, is not expected to carry all the load in creating and preserving evidence of authenticity.

The emergence of closed trading environments on the Internet belies the rationale made for the Utah Digital Signature Act that in an "open system like the public Internet" a digital signature is the only good way to establish that an identified person approved a message.

After my presentation one question raised from the floor was whether unsophisticated juries will assign to certification authorities and cryptographic algorithms the same weight and respect that the Utah government does in its Digital Signature Act. (See proposed Utah rules for certification authorities, <http://www.commerce.state.ut.us/web/commerce/digsig/rule.htm>). In other words, Will a jury of 12 people off the street really hold Grandmom to a contract that is mathematically signed by her private key, even though she repudiates it? I believe that is a legitimate concern, and it points up a risk for people who adhere to the Utah vision, that is people who rely exclusively on evidence created by cryptographic algorithms and make little effort to obtain or consider environmental

and circumstantial evidence.

Another question, raised during the break after my remarks, was whether it is easy to steal biometric information about one's signature from the PenOp system. For instance, couldn't someone simply clip the wire that connects a digital tablet to its host computer, insert an eavesdropping computer in the middle, and steal biometric information as it runs from the tablet to the host? The answer is that is harder than it looks. The communication between the tablet and its legitimate host can be protected by cryptographic, physical and other procedures. In the end, however, the biometric approach does not in and of itself supply absolute proof of signing and absolute protection from abuse. It can only provide relatively useful evidence that must be evaluated in the context of the computing environment and all the other surrounding facts and circumstances.

========

Benjamin Wright <Ben_Wright@compuserve.com> is an attorney and author of *The Law of Electronic Commerce,* published by Aspen Law & Business. This article is not legal advice for any specific situation. <http://infohaus.com/access/by-seller/Benjamin_Wright>.