Rafael Hirschfeld (Ed.)

Financial Cryptography

First International Conference, FC '97
Anguilla, British West Indies
February 24-28, 1997
Proceedings

Springer

Digital Signatures Today

A. Michael Froomkin

University of Miami School of Law
froomkin@law.miami.edu

Abstract. To a lawyer, two issues stand out as critical impediments to the widespread acceptance of digital signatures in electronic commerce: the unresolved nature of liability issues and the looming uncertainty about the nature of the public key infrastructure. These issues are so closely related as to be almost intertwined.

1 Liability

Although a few U.S. states have passed statutes addressing some liability issues relating to digital signatures, it remains safe to say that in most jurisdictions all or almost all liability issues remain murky. Certainly, in any U.S. state that lacks a digital signature law, it is highly uncertain who is responsible if a transaction backed by digital signatures goes wrong, especially if the authenticity of the signature, or the accuracy of a certificate, are called into doubt [2].

Suppose, for example, that Alice convinces a Certificate Authority (CA) to issue her a certificate falsely identifying her as Bob. Bob uses the certificate to defraud David. What happens? The short, depressing and—when it comes to transactions—inhibiting, answer is that we do not know with sufficient certainty to make a decent business plan, much less buy the right insurance.

First, if all participants live in different jurisdictions, it will often be unclear which jurisdiction's laws apply. In part this difficulty arises because we have no precedents as to which of the jurisdictions are most closely related to the transaction. In part, also, we have no certainty as to the ability of the CA to impose the choice-of-forum (if any) in its terms of service onto third parties.

Second, if the forum is a common law jurisdiction, we face the problem that there is likely to be no consensus as to the proper rule to apply. Suppose the CA was merely negligent rather than having colluded with Alice. Different states fall into three camps, each with a different rule concerning the liability to third parties such as David for the negligent misstatement concerning Alice's identity: one rule says he can collect, another says he ordinarily cannot, and reasonable people can disagree as to how the third rule could be applied to a CA—and that is the one which predominates.

Worse, it is unclear whether it is even possible at this early date to speak coherently of a CA's "negligence" (as opposed, say, to "gross negligence"—lawyers

 This essay is a slightly expanded version of remarks delivered at Financial Cryptograpy 1997.

can usually identify that and make you pay for it). In law, negligence is the failure to exercise "due care". In the absence of standards and practices for CA's, at this early and frankly experimental stage in the evolution of digital commerce and its certificate infrastructure, it is difficult to identify what constitutes reasonable care, and which violations of ideal procedures would amount to a violation of it. Exactly how closely should that CA's clerk have scrutinized the passport in the name of "Bob" tendered by Alice?

Worse still, it is not absolutely certain that the negligence paradigm is the appropriate one to apply to the issuers of certificates; whether appropriate or not, it may not be the one that the legislatures choose. Some law and economic based theories of tort suggest that costs of loss should be placed on the "least cost avoider"—the party who was best placed, ex ante, to prevent the loss. For an erroneous certificate, this will almost certainly be the CA in every case. Understandably, CAs may fear the consequence of strict liability for an erroneous certificate as it makes them virtual insurers of digital identity.

Similarly, the least cost avoider for the loss of control of a digital signature (or a private key) is the "subscriber," the owner of that data. All the other participants in a world of electronic commerce are likely to take comfort from a rule that allows them to rely on a digital signature supported by a valid, and verifiable, certificate [1]. Here, however, the subscriber will in many cases be a consumer, and the thrust of consumer law in many countries is to protect consumers from the natural consequences of their folly. If nothing else, this introduces another level of uncertainty.

The plethora of jurisdictions, with a plethora of different rules, each bearing different content and different quanta of uncertainty, is itself a major impediment to the widespread adoption of digital signatures in electronic commerce. Matters are not helped by the lack of standards among the issuers of certificates; having navigated their way throught the legal tangle, both users and issuers of certificates must then confront the fact that anything more than a simple identity certificate comes with long, complex, non-standard policies attached.

It is heartening to hear that various international bodies such as UNCITRAL are seeking at least basic harmonization of national rules; it remains to be seen whether either the U.S. states can harmonize their rules through institutions such as the Commissioners on Uniform State Laws, or whether in the end the federal government will have to adopt a national set of rules. Even so, the standards issue remains.

2 PKI Issues

Although not absolutely necessary for digital commerce to develop, a national or even international public key infrastructure (PKI) would obviously be a valuable tool for digital signature and certificate-based commerce. The development of a useful PKI is, however, complicated by several factors, including disagreement about the optimal shape of the hierarchy, political issues traceable to national

governments' desires to maintain their surveillance and/or export control rules, and the general lack of standards for the form and content of certificates.

There appears to be disagreement as to what the ideal certificate infrastructure should look like. Some, coming from one well-known standards tradition, favor a single highly hierarchical system; others, perhaps thinking about deploying more quickly, advocate or predict a number of flat hierarchies. Although no expert myself, it seems likely to me that in the absence of government intervention at least in the short term the commercial pressure will be to flatter and complementary, albeit also sometimes competing, certificate hierarchies.

Government intervention, however, seems quite likely. Although it is early days, so far what we have seen of proposed national PKI policies, particularly the U.S. so-called Clipper 3.1 White Paper [4], seem driven more by law-enforcement concerns than by the needs of the digital marketplace. While a national system may resolve the easy issues of root certification, the harder issues of hosting a large and ever-changing database, or even the very difficult issues of participant liability, the proposals on the table appear likely to introduce new classes of problems. Since these issues are familiar to this audience, I will limit myself to brief mention of two: the issues of "key escrow" and anonymity.

Most governments that have spoken on the question, including the US government, have made it clear that they do not seek to "escrow" authentication (digital signature) keys, but only keys used for communication. The problem, of course, is that signature keys can be used for communication, either directly or to enable authenticated Diffie-Hellman key exchange. This risks creating pressure for the "escrow" of signature keys also. That, of course, would be unjustified and might well undermine confidence in the PKI. It would certainly make me more reluctant to use it, since anyone able to access the "escrowed" data on my signature key would have a way of signing my supposedly unforgeable signature to absolutely anything. Escrow also risks added expense and complexity that may make a PKI more difficult.

Anonymity presents an important but less publicized issue. I have argued that the growth of profiling technologies will make anonymous communication more and more important to the average consumer/citizen: anonymity may become the only practical means of preserving one's privacy against profilers [3]. It is not at all clear that government-backed proposals for a PKI will be friendly to anonymous identities. Indeed, if a design goal is to be make it possible for law enforcement to link identities to keys, there will be no space for anonymously or even pseudonymously held keys. If electronic commerce and web-based media should become the dominant means for the exchange of ideas, the issue of preserving a space for anonymous communications may take on great importance.

3 A Final Thought

In conclusion, I would like to reiterate a point I made earlier: of all the impediments to the spread of electronic commerce based on digital signatures that I have discussed, one stands out as being solvable by the people here today, and

that is the absence of international standards for the representations contained in certificates. At present, there is not even a standard syntax in which these policies could be stated; as a result, there is no hope of automating or even partly automating the problem of what certificate to accept. Instead, each type of certificate offered by each issuer must be manually scrutinized—and perhaps referred to counsel—before a decision can be made as to whether to rely on it. Here is work to be done that could in turn create the conditions to begin to solve many, although not all, of the other problems I have outlined.

References

1. American Bar Association, Information Security Committee, Section on Science and Technology, Digital Signature Guidelines (1996).
2. A. Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Oregon Law Journal 49 (1996).
3. A. Michael Froomkin, Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases, 15 Pitt J L & Commerce (1996).
4. Bruce W. McConnell & Edward J. Appel, Co-Chairs, Interagency Working Group on Cryptography Policy, Draft Paper: Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure ("White Paper") 23 (May 20, 1996), available from Office of Management and Budget, Executive Office of the President), and online at `http://www.isse.gmu.edu/~pfarrell/nist/kmi.html`.