International Lawyer

Volume 32 | Number 4 Article 3

1998

International Developments Affecting Digital Signatures

Stewart A. Baker

STEWART A. BAKER*

International Developments Affecting Digital Signatures

An old encryption technology invented to lock away information may now be the key to opening the Internet to international commerce on a grand scale. Digital signature technology provides a simple and secure means of authenticating electronic documents. This is a critical step toward making the Internet a safe and reliable environment in which to conduct electronic transactions. Governments and international bodies have been scrambling to establish legal regimes to govern digital signature transactions in anticipation of the inevitable deluge of electronic transactions that will arrive as a result of the technology. Unfortunately, those governments that have examined the question have passed digital signature legislation with little regard for legislation passed in other countries, thus creating an international patchwork of regulations that will surely inhibit rather than catalyze cross-border electronic commerce. Moreover, many national and state governments have enacted laws that dangerously over-regulate digital signature transactions, pay insufficient attention to the use of electronic signature technologies other than digital signature technology, disregard the use of private digital signature commercial networks, and overlook the importance of low-security electronic transactions. The United States should take a leading role in establishing international standards for digital signature transactions that address these concerns and rescue digital signature technology from a premature demise.

Over the past three years there has been an explosion of legislative activity relating to the regulation of electronic signatures, with particular emphasis on digital signature infrastructures. The State of the Utah has been at the forefront of the digital signature shock wave. In 1995, Utah enacted one of the earliest, and most comprehensive, laws authorizing the commercial use of digital signatures.[1] At least thirty other states have passed some form of legislation regarding the use of electronic or digital signatures, and in at least eight other states,

*Stewart A. Baker is a partner at Steptoe & Johnson LLP in Washington, D.C.

1. Utah Digital Signature Act, UTAH CODE ANN. §§ 46-3-101 to 46-3-504 (1995).

proposed electronic and digital signature laws are moving through the legislative process.[2] In the past few months, bills have also been introduced in Congress dealing with digital and other forms of electronic signature.[3] Recently, a number of foreign governments have also enacted—or are seriously considering—electronic and digital signature laws.[4]

As is evident from the amount of attention being given digital signatures by legislatures around the world, this technology is popular. Oddly, its popularity is the biggest obstacle it faces. Digital signature technology may be loved to death before it ever gets an opportunity to really take off.

I. The Technology

Generally speaking, cryptography entails the enciphering of a message into a form unreadable to anyone not possessing the key to decipher the message. Conventional cryptography involves a single mathematical key, known only to the sender and recipient of an encrypted message, which is used by the sender of the message to encrypt a message and by the recipient to decrypt it. "Public Key Cryptography," first described publicly in 1975, is a special method of encrypting and decrypting messages by means of a pair of mathematically-related keys. This method involves two keys: a "public key" known to one or more parties and a "private key" known only to a single party. Either key may be used to encrypt or decrypt a message.[5]

In essence, Public Key Cryptography relies on the difficulty of reversing certain mathematical functions. For example, multiplying to find a product is easy; factoring to find the numbers that were originally multiplied together is hard. With big enough numbers, one number may be kept secret and the other number may be published without any fear that the secret number can be guessed by an adversary. Thus, everyone in the world can look up the public number and use it to encrypt a message that only the author can read.

2. States that have passed some form of legislation regarding digital or electronic signatures include the following: Alabama, Alaska, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. Most of the digital or electronic signature legislation passed by states so far is limited in applicability, though, to transactions with state agencies; few states have been bold enough to validate the use of digital or electronic signatures in all commercial transactions. States still considering legislation regarding digital or electronic signatures include the following: Maryland, Massachusetts, Michigan, New Jersey, New York, North Carolina, Pennsylvania, and Vermont.

3. Digital Signature and Electronic Authentication Law of 1998, S. 1594, 105th Cong.; Electronic Financial Services Efficiency Act of 1997, H.R. 2937, 105th Cong.

4. These countries include Argentina, Canada, Germany, Italy, Japan, Malaysia, Singapore, and the United Kingdom.

5. Computer hardware and software using two keys for encryption and decryption are referred to as an "asymmetric cryptosystem."

That is the part of the public-key revolution that gives the FBI and the National Security Agency nightmares.

But the flip side of that process is just as intriguing—and may become the predominant use of public-key technology: If I encrypt a message with my private key, anyone in the world can decrypt it using my public key. This is no way to keep secrets, but it is a great way to tell the world that only I could have sent the message. Since I am the only one in the world who knows what my private key is, no one else could have written a message that can be decrypted using my public key. In short, encrypting a message with my private key acts like a "digital signature," identifying me as the source of the message.

The advantages of this technology for cyberspace are obvious. It allows highly sensitive material to be put on a network with access restricted by the requirement that users sign in digitally using their private keys to encrypt messages that can be checked against their public key. In fact, with only a modest infrastructure, strangers can do business with other strangers all across the globe by using a few digital signatures to establish their bona fides.

But how does the recipient of a digitally-signed message know that the identity he believes to be associated with a certain public-private key pair really is associated with that key pair? What is needed to make this scenario possible is a set of rules and procedures for certifying the authenticity of digital signatures so that message senders and recipients can act with confidence. Such a system of rules and procedures is called a Public Key Infrastructure (PKI).

In the simplest case, suppose a bank issues digital signatures to each of its customers who have maintained a $10,000 checking balance over the past year. If I want to do business on-line with another customer of the bank and he sends me a copy of his bank-issued digital signature, I can be pretty sure that his $5,000 offer is good. As a practical matter, the bank would probably issue a public-private key pair to its customers and then tell them to store the private key somewhere safe (a 3½-inch floppy would be good; a chip card would be better). The bank could publish the customer's public key (as well as its own) on the Internet and elsewhere. However, since the bank will not want to identify its clients as targets for scams or worse, it is more likely that the bank will privately issue an electronic certificate that says, "As of October 1, the holder of this private key has maintained a $10,000 checking balance for the past year, signed, His Bank." The customer can then send that certificate to people who need to know his credit is good, and they can rely on it as long as they know the bank's public key (needed to decrypt the bank's certificate) and trust the bank to tell the truth.

How, in practice, do you actually create a digital signature and attach it to a message? You can acquire commercially-available digital-signature software capable of generating a public-private key pair, or you can ask a certifying authority to do that for you. Once you have a key pair, the certifying authority must issue a certificate vouching for your identity and ownership of the public key in question. The certifying authority then places this certificate in an on-line reposi-

tory, where it can be viewed by anyone to whom you might send a digitally-signed message. Now you can begin sending messages. The sender first composes a message. Then, the sender activates the digital-signature software by clicking on an icon on his computer screen. The sender is prompted to introduce his private key, which is typically stored on a "cryptographic token," such as a 3½-inch floppy disk or "smart card." Ideally, the digital-signature program is executed within the cryptographic token, so that the private key never migrates into the memory or processor of the sender's computer where it could be copied or stolen. The software runs the text of the message through a mathematical algorithm which generates a short jumble of numbers and letters called a "hash code." Each message has a unique hash code. The digital-signature software then encrypts the hash code using the sender's private key. The result is another short jumble of numbers, letters, and symbols appended to the bottom of the message: a digital signature unique to the accompanying message.[6] The recipient uses the same software to decrypt the digital signature by reference to the sender's public key. A successful decryption verifies that the message was in fact sent by the person whose identity corresponds to the public key. The software then passes the received message through the same algorithm and compares the resulting hash code to the hash code encrypted into the digital signature. If the two hash codes are the same, the recipient knows the message was not altered after it was sent; its integrity has been preserved. The sender will also have a difficult time denying that the message was sent by him, i.e., repudiating the message.[7]

II. Why the Technology Requires New Legal Rules

The efficiency and security that this system allows are tremendously exciting, but a few problems still exist. First, suppose the customer is sloppy with his private key. He writes the password to his smart card on the card and then leaves the card in the washroom. Now anyone who has the card can use his identity—and his credit. To deal with that problem, the bank needs to maintain an easily accessible list of stolen or compromised public-private key pairs. This is known as a Certificate Revocation List (CRL). To make the system work, however, anyone who relies on digital signatures must know about and regularly check the CRL.

But this is the real world. Some people will not check the CRL. They will get burned. They will blame the bank because it has the most money to pay damages. They will sue.

Without a law on digital signatures and certificates that apportions liability among the various parties involved in an electronic transaction (comparable to

6. A digital signature, appearing as an encrypted alphanumeric code, should not be confused with a digitized signature, which is an electronic representation of the sender's actual written signature.

7. Most laws regulating the use of digital signatures require that a digital signature ensure, at a minimum, authentication of the identity of the sender of a message, message integrity, and message nonrepudiation.

the banking and checking provisions of the Uniform Commercial Code), no one knows how such a suit will come out. The bank can write a contract with the customer that demands he be careful with his private key and perhaps even makes him liable for his negligence. But consumer groups would oppose enforcement of such contracts (digital signature buffs call this the "Grandma picks a bad password and loses her house" problem). Even worse from the bank's point of view, it does not have a contract with the person who got burned by the compromised signature. He is just an innocent third party who lost money—by relying on the word of the bank, his lawyer will argue.

Without more legal certainty about how to protect themselves (or how much insurance to buy), companies with deep pockets will not want to take that risk. They will stay out of the business of issuing digital signatures and digital certificates for such transactions. In fact, for a decade or more, that has mostly been the story: Cool math confronts corporate legal department; cool math loses.

III. How Digital Signatures Are Actually Being Implemented Today

The technology is too good to be locked up by lawyers forever. Companies that wanted to use digital-signature technologies began looking for places where this open-ended liability was not a big problem. They found at least two.

A. Cheap Certificates

First, companies offered certificates paired with a sweeping disclaimer of any liability. These certificates are not suited for high-value transactions, but they can be used in a lot of circumstances where even a no-liability signature is better than no signature at all.

Millions of cheap, liability-free certificates are already in circulation. Some certificates, for example, do little more than confirm that a given user's name corresponds to a particular e-mail address, as determined by examination of the register maintained by the certifying authority; such certificates do not authenticate the identity associated with a digital signature. Though helpful, such certificates would not afford the level of security desired by the parties to a high-value electronic transaction. The secure socket layer (SSL) encryption that everyone uses for secure web connections also relies in part on digital signatures to identify the server and the browser to each other. No one really guarantees the server's public key, but if it is the same one every time I log on, I can be fairly sure that I am dealing with the same server, belonging to the same store, rather than to an on-line con-artist. Other Internet-based cheap certificates include the "authenticode" certificates used to identify the authors of Java-like ActiveX programs. The "authenticode" certificates offer a modest, but better-than-nothing, security precaution for Internet users who are understandably reluctant to let codes written by strangers gain access to their computer's operating system.

B. Closed System Certificates

Second, some digital-signature proponents have begun creating what amounts to their own law, by contract. Any group of companies or individuals may, of course, do business in accordance with one or more agreements setting forth the liability and other rules that govern their relationships; such closed communities can create a self-contained set of rules to cover digital signatures. IBM, for example, can issue digital-identity certificates to all of its employees; it can say that they are good for e-mail attribution and for petty cash requests but not for private transactions unrelated to work—or whatever rules that IBM is comfortable with. Or, in a more exciting use, Visa can issue certificates to all of its member banks, and they can issue certificates to all of their cardholders and merchants. Suddenly, shoppers don't have to type their credit card numbers on the screen at Amazon.com, and they do not have to worry about Internet card number theft.

Within the preexisting Visa relationships, all those tough liability problems become easy. Visa simply says that using a digital signature will not substantially change the existing liability rules for any of the system participants. Liability is already covered by an elaborate set of agreements and rules, some driven by long-standing government regulations. (Remember Grandma and her house? For credit cards, the rule is clear inside the United States: if she picks a bad password, she may lose fifty bucks but she will not lose her house.) In fact, Visa and Mastercard have built digital signatures into a Secure Electronic Transaction protocol (SET) that is already being implemented in several countries.[8]

IV. Lawyers to the Rescue?

While all of this was going on, the lawyers themselves began to look for legislative solutions. In 1995, a committee of the American Bar Association led by Michael Baum (now the top lawyer at VeriSign) designed a comprehensive model law to deal with all the new legal issues arising from digital signatures. While that work was underway, the state of Utah took the plunge, enacting a variant of the ABA draft. Within three years, more than forty state legislatures were contemplating digital signature laws. So were numerous countries; indeed, by the fall of 1997, Germany, Malaysia, and Italy already had their own laws, and many more bills were in legislative hoppers around the world.

8. On October 14, 1997, VeriSign, a company specializing in software for use in secure electronic transactions, announced that it would issue a new type of digital identifier for banks and financial institutions interested in doing business over the Internet. The new digital certificate, called Financial Service ID, vouches for the identities of banks, brokerages, and pension funds that support the Open Financial Exchange specification created by Microsoft, Intuit, and CheckFree for home banking services. The special digital certificates will be restricted, however, to large financial institutions. VeriSign already issues several personal digital IDs to Internet users and offers digital certificates for banks, merchants, and individuals under the SET protocol. *See* Tim Clark, *Locking Up Home Banking* (visited Oct. 14, 1997) <http://www.news.com/News/Item/0,4,15222,00.html>.

This should be good news—lawyers and lawmakers working together to solve a legal problem and enable the birth of a new technology. But it is not. As we will see, it is posing a growing threat to the burgeoning use of low-value certificates and closed certificate systems.

Digital signature laws are often sold to legislators as a way to bring written signature requirements into the computer age. An image is conjured up of digital signatures being rejected by courts insisting on something executed with a quill pen. This is an overstated problem, at least in the United States and for most commercial transactions. Courts have, after all, been treating printed telegrams as signed documents for a century. There is nothing about a digital signature that makes it a harder legal problem than telegrams—or telexes, or typed letters, or faxed signatures, or a dozen other ways in which real-world commercial actors have lawfully signed contracts over the last century.

What digital signatures need—uniquely—from the law is certainty about the obligations and rights of three parties:

(1) the keyholder who is identified by the public key and who controls the private key,
(2) the certifying authority (CA) who vouches for the public key and ties it to the identity (or creditworthiness, or chess club membership, or whatever) of the keyholder, and
(3) the relying party who gets the public key and the certificate and decides to trust the certificate.

The Utah law, and the ABA guidelines, decided to spell out all of these duties in great detail. In particular, to make sure that relying parties could trust CAs, the Utah law and the ABA called for government licensing. The government would make sure that prospective CAs are trustworthy and that they remain so. It would check the technical and other security measures that CAs use to protect keys and would enforce rules about documents CAs should demand before certifying someone's signature. (Can the CA issue an identity certificate based on one piece of identification or must it see three? Does it have to check the keyholder's address? And so on.)

For the most part, the Utah bill is also pretty tough on keyholders. If they are not careful with their private keys, they will lose their houses. Early boosters of the technology, however, thought the alternative was worse: Relying parties and certifying authorities might refuse to participate in digital signature transactions if keyholders could invalidate transactions after the fact by making up a story about having been negligent with their keys.

V. How Many Lawmakers Does It Take to Screw Up an Infrastructure?

Two problems with the Utah approach only became apparent as digital signature laws began to sweep through legislature after legislature.

A. Conflicting Obligations

First, not every lawmaker saw the policy issues in the same way as Utah lawmakers. And the more detailed the legislation, the more room there was for fatal conflicts between state laws, sometimes on the most inconsequential points.

For example, both Utah and Washington require a CA to suspend a certificate if the CA gets a call from the keyholder saying the private key has been compromised. (In Utah, the keyholder has a big incentive to act fast; he wants the compromised key suspended before somebody sells his house.)

But to guard against fraud or pranks ("Hey, guys, let's call up the bank and suspend our gym teacher's public key."), the CA cannot suspend the key for long without checking to make sure that the suspension request really came from the keyholder. Under Utah law, the check has to be done within two days, but the certificate is automatically suspended whenever the CA gets a request from someone claiming to be the keyholder. Under Washington law, the caller can ask for a four-day suspension, but the CA can only suspend the certificate if the CA is pretty sure that the caller really is the keyholder.

Same basic idea in both states. But what if you are a CA doing business in both states and you get a suspension request from someone who does not sound very much like the keyholder? In Utah, you must suspend; in Washington, you cannot. Or suppose the caller asks for three days to come in and verify his identity? In Utah, you cannot wait that long; in Washington, you must. CAs simply cannot obey the laws of both states.

Other states have tried to avoid such problems by writing less detailed laws, leaving a lot to regulatory authorities. But that just postpones the conflicts, and perhaps makes them harder to find. It does not eliminate the likelihood of conflicting regulations. After all, many of the questions addressed by the Utah law have no easy answer. How much risk should the keyholder bear and how much should fall on the CA? Different states, and certainly different countries, will arrive at different answers to such questions. But if CAs must change their practice in each country or each state, there will be very few CAs in ten years, and digital signatures will not live up to their promise.

B. State Licensing

An even bigger potential problem is the solution Utah used to ensure the quality of CAs. Having CAs obtain licenses from the state in exchange for accepting regulation by the state is very appealing in many ways. Licensing is flexible, allows the state to "back up" the digital signature of a licensed CA with a state-issued certificate, and gives unhappy parties somewhere to go with complaints.

But what if licensing is mandatory? Suddenly, many cheap but useful certificates could become too much trouble to bother with. Take the example of a merchant who wants to improve on-line shopping security by issuing customer certificates: "This certifies that the holder has purchased more than five books

at Amazon.com using the name 'Stewart Baker'." If Amazon.com cannot issue a simple customer certificate without registering in fifty states and complying with all of the security rules that apply to the high-trust certificates, it will just stop using certificates like this. And we will all have a little less security when we shop on-line.

So far, in the United States, licensing has remained voluntary. If a CA wants the imprimatur of the state of Utah, it must register there. If not, not. Either way, the CA can lawfully issue certificates to Utah residents. Actually, there are still some disadvantages that will push many firms into registering in most states, but I am ignoring them for simplicity.

This is not so abroad. Germany's law contains no savings clause for cheap certificates. It implies that no one may issue certificates without meeting strict standards for security; these standards include a requirement that private keys be stored only on a smart card—they cannot be sent over the Internet, and they cannot be stored on a magnetic stripe card or 3½-inch floppy.

If pressed, German authorities sometimes say that they will not punish those who issue unauthorized certificates. That seems to be what they are telling the European Commission, which is worried about the trade-restricting impact of the German law. But privately, some officials say that within three years the licensing regime will be mature and unauthorized CAs will be stamped out.[9]

In Malaysia, that future is now. Malaysia's recently enacted digital signature bill makes it clear that anyone who issues certificates must register in Malaysia.

And it is not just cheap but useful certificates that will be affected. SET, arguably the most sweeping and important use of digital signature technology to actually see the light of day, is also harmed by the proliferation of registration requirements. Neither Malaysia nor Germany was willing to make a clear exception in its law even for entirely private and consensual uses of digital signatures.

VI. Why Conflicting Rules Will Not Go Away by Themselves

What is going on here? Partly, of course, it is just that some governments choose regulatory solutions for everything. In Europe, the idea of letting market forces act is viewed with suspicion in the best of times. It sounds even less plausible coming from the same Internet advocates who cheerfully proclaim that national borders are just speed bumps on the information highway and that important national policies—on distribution of pornography, on wiretapping, and a host of other issues—will soon be rendered unenforceable by a global market.

9. On December 19, 1997, Germany's Office for Information Security announced it would review and possibly revise its proposed technical specifications for digital signatures and CAs. *Germany's Proposed Technical Specifications for Digital Signatures, CAs to be Revised*, ELECTRONIC INFO. POL'Y & L. REP. (BNA) 8 (Jan. 7, 1998). The German technical specifications, published in a book over 300 pages long, were widely criticized for requiring a very high level of security and for being over-regulatory, much too complicated, and inflexible. *Id.*

Worse, many other nations fear that such statements are just a disguised bid for American domination: "Leave it to the market, where our companies have an enormous lead." So government regulation looks to these nations as a cheap way to even the odds; whatever competitive problems local technology companies may have in other arenas, they surely know more than Americans about working successfully with local authorities.

The case for regulation gets stronger as the stakes get higher as well. If the main use for digital signatures will be for a national identity card that includes bank account access, the companies issuing those certificates should be watched closely. If legislators do not know much about other uses of digital-signature technology, or if a digital-signature law is being jammed through the legislature by a few interested parties under the guise of modernizing signature requirements, it is not likely that closed systems or low-value certificates will get much attention from the legislative drafters.

Whatever the motivation for this outburst of regulatory zeal, the results will likely be a disaster for implementation of a public key infrastructure. Even if they might be able to get an exemption from most laws, users and issuers of cheap certificates cannot bear even a remote prospect of liability in a handful of countries. Rather than register, they will find weaker, less-regulated alternatives to digital signatures—or they will do without entirely. The same goes for "closed system" users of digital signatures. Burgeoning regulations that are not tailored to their private certificate system will create disincentives for credit card companies to use digital signatures. In short, this outbreak of regulatory enthusiasm is likely to make digital signatures much rarer and much riskier for prospective certificate authorities.

The next question is what U.S. policymakers should do to avoid this train wreck. Inside the United States, efforts to write a uniform state law that would resolve some of these issues are moving forward, but slowly. There are honest disagreements about how much liability to assign to the parties to a transaction and how much freedom of contract should be recognized in a complex field with major implications for consumers. So even if a uniform law is agreed upon, it may not exactly sweep the nation.

That is why there is support for at least a limited form of preemption by the federal government, perhaps just a list of things that states will not be allowed to do such as imposing their rules on otherwise valid "closed" systems or requiring issuers of even low-value certificates to register as CAs. These restrictions might be enough, for example, to reassure financial institutions and others that they can use digital signatures to secure payment systems without fear of being surprised by newly imposed state liabilities.

At the international level, the U.S. government has stated its support for the establishment of a Global Information Infrastructure (GII)[10] as a means of promot-

10. *See* The White House, *Framework for Global Electronic Commerce* (visited Sept. 21, 1998) <http://www.ecommerce.gov/framewrk.htm> (Administration's recent White Paper on the GII).

ing trade and commerce, especially electronic commerce. Such an ambitious objective, however, would necessarily require the harmonization of world legal norms governing the use of digital signatures, as the number of transactions involving digital signatures can only be expected to grow. Persuading other countries to adopt the same rules usually requires lengthy bilateral or multilateral negotiations resulting in a treaty or other agreement. But there are at least two other models as well.

A. OECD

The Organization for Economic Cooperation and Development (OECD) specializes in nonbinding, consensual codes of conduct and guidelines. These codes and guidelines are developed by the world's richest nations to coordinate policies on a variety of topics from privacy to cryptography.

The OECD has recently released a paper on issues raised by international certification of digital signatures, and it shows some of the OECD's strengths and weaknesses as a forum. To bolster its claim that it should address the digital signature issue, the OECD notes that it has already done extensive work on privacy and on cryptography guidelines. The report suggests that both are related to digital signatures because digital signatures allow extensive tracking of individuals and because the technology is closely tied to encryption and the law-enforcement-access debate that dominated the OECD's deliberations on cryptography.

This observation is a distinctly two-edged sword for OECD. Both the privacy and the cryptography guidelines were a source of continued and bitter controversy. Digital signatures do not have to be dragged into either debate, but handing the problem to the OECD more or less guarantees a replay of past three-way battles between government, industry, and privacy advocates.

B. UNCITRAL

The United Nations Commission on International Trade Law (UNCITRAL) plays a consensus-building role for a larger audience—UN members. In addition, its products tend to be more specific and less controversial, focusing on achieving technical consensus on the language of model laws or conventions to regulate aspects of international trade including international arbitration, international sale of goods, and the like.

UNCITRAL already has a concrete record of achievement on technical legal issues affecting digital signatures. It has released a model law on electronic commerce, the 1996 UNCITRAL Model Law on Electronic Commerce (Model Law), which reflects the contributions of more than fifty countries over a three-year period. The Model Law, which has also been endorsed by the UN's General Assembly, treats digital (and other electronic) signatures attached to a message as valid and binding, so long as the method of signing was "as

reliable as appropriate for the purpose for which the data message was generated or communicated."[11]

Although the Model Law itself lays to rest any questions about the validity of digital signatures for purposes of commercial transactions, UNCITRAL recognized that digital signatures and PKI raise legal issues going well beyond this point. For that reason, UNCITRAL's Working Group on Electronic Commerce (Working Group) has already begun work on a set of Uniform Rules to deal with certification authorities and the problems relating to the recognition of foreign electronic signatures. Unfortunately, the work done so far suggests that UNCITRAL's efforts could easily fail to produce a consensus. Thus, it is not clear that the UNCITRAL efforts will in fact provide the kind of relief and assurance of legality needed by producers of low-value certificates and closed systems that use digital signatures.

The draft produced early in 1997 by an UNCITRAL Working Group on certification authorities was clearly cast in the "high-value, government-regulated" mold. It envisioned "authorized" certification authorities meeting detailed state standards, and it was fairly prescriptive with respect to the nature of the certificates issued. For example, the draft would have required that any certificate issued by a CA state the identity of the party receiving it. This is difficult if the certificate is to be used to identify software or servers, and it is even imprudent in the context of credit cards. Credit card companies generally resist allowing the use of their cards for general identification purposes; the credit card companies are more interested in verifying creditworthiness than identity.

More recent meetings have resulted in new drafts that limit the most heavily regulatory language. But at least Germany—and perhaps other European nations—remain wedded in varying degrees to the notion that certification services are too important to be left to the private market. What is more, the Europeans have shown only modest sympathy for private, closed systems using digital signatures and virtually none for issuers of cheap certificates.

UNCITRAL is, in the end, a consensus-driven body, and it is clear that no consensus will be reached if low-value and closed-system certificates are not recognized in some fashion. But consensus runs two ways. Supporters of regulation may well insist that the final draft also endorse a highly regulatory scheme. Perhaps some method of accommodating both systems can be found. If not, the consensus process will fail. The UNCITRAL process may not be able to broker serious differences among nations.[12]

---

11. United Nations: UNCITRAL Model Law on Electronic Commerce, Dec. 16, 1996, art. 7, 36 I.L.M. 197, 204 (1997).

12. The UNCITRAL Working Group on Electronic Commerce was to meet in session again in November 1998.

VII. Which is the Right Forum?

Unfortunately, it is becoming increasingly likely that serious differences will arise internationally between countries enamored of the high-regulation, high-trust model and those more open to market developments in digital signature use. This opens the door to protectionism and discrimination. Germany has already enacted a law that automatically recognizes equivalent signatures from other EU countries, but says that recognition of U.S. signatures will have to wait for the negotiation of a bilateral or multilateral agreement. France has announced that for national security reasons only French-owned companies may serve as the trusted third parties who will be CAs in France. Italy reserves a special place among CAs for Italian notaries.

UNCITRAL is an unlikely place to combat such tendencies. It does not have a tradition of brokering trade disputes. The OECD is a more plausible forum for addressing such differences, but its process yields only guidelines, not binding agreements.

Are there other fora? Perhaps. The WTO does have some claim to jurisdiction over trade in services but it lacks a clear framework for resolving this matter. More interestingly, the U.S. Government and the European Commission—usually antagonists on trade—may have some common interests here. Both are concerned that excessive regulation of digital signatures will lead to inconsistent standards and discrimination within their boundaries. And both have been a bit left out as their constituent parts raced to define new regulatory schemes. While there are pitfalls, the United States and the European Union might be able to reach a quick understanding on at least some basic rules to discipline the digital signature laws of their constituent states.