4005 Miranda Avenue
Suite 175
Palo Alto, CA 94304
415.858.1930

fax: 415.858.1936
E-MAIL:
info@commerce.net
http://www.commerce.net

Statement
on
Certificate Authorities and Digital Signatures

for the

U.S. Department of Commerce
Public Forum on Certificate Authorities and Digital Signatures:
Enhancing Global Electronic Commerce

July 16, 1997

CommerceNet is the leading industry consortium dedicated to accelerating the growth of Internet commerce and expanding Internet markets. Launched in California's Silicon Valley in April 1994, CommerceNet's membership has grown to over 150 leading organizations in areas such as banking, electronics, computers, online services, information service industries, as well as major end users. Together, we are transforming the Internet into a global electronic marketplace.

CommerceNet appreciates the Department of Commerce's interest in enhancing global electronic commerce and specifically in certificate authorities and digital signatures. We appreciate this opportunity to provide the Department of Commerce with input on this subject, which CommerceNet sees as an essential building block to electronic commerce.

Uniformity

CommerceNet is an official observer to the NCCUSL Drafting Committee on a Uniform Electronic Communication in Contractual Transactions Act and has been active in the drafting process for some state laws and regulations.

Traditionally, contract law, including law dealing with what constitutes a signature, has been a matter for which the states have taken responsibility. As noted in the Department of Commerce notice for this forum, some two dozen states have passed some form of "digital signature laws" in the last two years. Significant efforts are being made to implement public key infrastructures. Some concerns have been expressed regarding possible negative effects of a multitude of inharmonious state laws. Indeed the National Conference of Commissioners on Uniform State Laws has also noted this concern and has created a Drafting Committee to address those issues.

CommerceNet believes that the states are capable of resolving these issues and that the Federal government should allow private and state interests to proceed until such time, if ever, it becomes apparent that Federal intervention is necessary to ensure any degree of uniformity necessary to ensure the smooth functioning of electronic commerce across multiple jurisdictions.

Reliability

CommerceNet is extremely concerned with both recently introduced legislation and the recent testimony of FBI director Louis Freeh[1]. The McCain-Kerrey legislation authorizes the Department of Commerce to license Certification Authorities but commingles the treatment of "encryption certificates" with digital signature certificates, and in so doing implies that a mechanism for the escrow of digital signature keys is desirable. We are further concerned that regulations may be put in place to actually require escrow of signature keys in order to obtain a signature certificate from a federally licensed certification authority, which in turn would be required to do business with Federal agencies. This would not enhance electronic commerce, but instead would make a mockery of it. In effect, the Federal government would be saying "We will allow you to do business with us electronically, but only if you give us the ability to sign the contracts for you." Whatever the intent of the legislation, its effect would be to decimate electronic commerce in its infancy. Mr. Freeh goes even further and states that escrow of digital signature keys should be mandatory. The U.S. public, which has strenuously resisted giving the government the unlimited ability to read private communications, is now being asked to give the government the ability to sign anyone's name to an electronic document. While there may be some argument to be made that law enforcement needs to be able to monitor communications in case one of the communicators is involved in criminal activity, there is no argument to be made that law enforcement needs to be able to sign (and arguably authenticate) documents in the name of other parties without the authorization of those parties.

In CommerceNet's opinion, the single most significant action that the Department of Commerce can take to enhance global electronic commerce is to oppose any legislation or regulation that would require or provide an incentive for the escrow of signature keys. It is our strong opinion that a signature created with an escrowed signature key is invalid and cannot be relied upon at all. Like a manual signature, a digital signature's primary value is in indicating the identity of the person that created it. If the private key, whose very possession suffices to authenticate identity, is disclosed to third parties who are not authorized to sign in the key holders name, then the very foundation of a reliable public key infrastructure is not only undermined but totally compromised.

Privacy and Identity

The role of Certification Authorities in electronic commerce is to ensure that a person or business can be reliably identified as a party to a transaction or communication. However, identification of parties inevitably leads to privacy concerns. CommerceNet believes that it is essential to properly balance individual privacy with appropriate protections for both consumer and business purchasers of goods and services effected by electronic commerce. When comparing individuals to businesses, we see significantly different requirements for the amount of information necessary to properly ensure authentication in electronic commerce. For the individual, privacy of personal information must be protected. On the other hand, for a business appropriate disclosure must be made so that customers are ensured that they can contact that business should problems develop in the delivery or quality of the goods or services purchased. Additionally, care must be taken

[1] Testimony before the Senate Judiciary Committee on July 9.

that a business can identify whether or not its customer is of legal age to enter into a valid purchase. The following principles should be followed:

- A digital certificate used to identify an individual should contain no more information than the individual desires to make available. Furthermore, the certificate holder should have control over what information he or she wishes to disclose in a given transaction or communication. However, the certificate should contain information on whether or not the individual is of legal age.

- A digital certificate used to identify a business should contain enough information to identify the physical location of the business.

CommerceNet believes that market forces and the necessity for Certification Authorities to hold themselves to high standards of protection of personal information will ensure that these principles are met. Unless and until the Federal government finds that these principles are NOT being met, the government should leave privacy standards for digital certificates to the private sector.

In closing, we suggest that the following principles, as detailed in the Administration's *Framework for Global Electronic Commerce*[2], should be followed in determining any Department of Commerce role in the development and deployment of Certificate Authorities:

1. The private sector should lead.
2. Governments should avoid undue restrictions on electronic commerce.
3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.
4. Governments should recognize the unique qualities of the Internet.
5. Electronic Commerce over the Internet should be facilitated on a global basis.

CommerceNet would be pleased to provide whatever further help the Department may find useful in defining its role in the development and deployment of an infrastructure for digital signatures. We encourage the Department to call on us whenever we can be of use.

Submitted by:
Kaye K. Caldwell
Policy Director
Direct Dial: 408-479-8743 Direct Fax: 408-479-9247
E-MAIL: KCaldwell@Commerce.net

[2] http://www.whitehouse.gov/WH/New/Commerce/read.html