Child Online Protection Act

TO: Commission on Online Child Protection

FROM: Michael S. Baum
Vice President, VeriSign, Inc.
michael@verisign.com

RE: Comments on Verification Systems

DATE: June 5, 2000

I. Introduction

This paper[1] responds to the Commission on Online Child Protection's (Commission) request for comments regarding "one-click away" resources, age verification systems, and an adult top-level domain in support of the Child Online Protection Act (COPA).[2] Specifically, it describes how digital signature technology might be used to support age verification systems under COPA.

This memo's main proposition is that only digital signatures[3] and supporting public key infrastructures (PKIs)[4] can provide adequate and scalable security for information

[1] This paper is available at < http://www.repository/pubs/copa >.

[2] 47 USC § 231.

[3] Digital signatures utilize a key pair consisting of a key that is kept secret by its holder (the *private key*) and a corresponding key that is (or can be) made public (the *public key*) without compromising the private key. To digitally sign a message, the signer applies his or her private key to it. The digital signature is not the private key itself; rather, it is a number, unique to that particular signed message, that is generated when the private key is applied to the message. Therefore, every digitally signed message contains a unique digital signature. It is computationally infeasible to ascertain a user's private key by evaluating a digital signature from one of his or her messages. See INFORMATION SECURITY COMMITTEE, SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE § 1.11 (1996), < http://www.abanet.org/scitech/ec/isc/digital_signature.html >.

[4] The term *public key infrastructure* refers "both to a certification infrastructure based on public and private cryptographic keys and to the discrete components of such an infrastructure, including certification authorities, certificates, digital signatures, and the hardware and software that implements the infrastructure." *See* Michael S. Baum & Warwick Ford, *Public Key Infrastructure Interoperation*, 38 JURIMETRICS J. 359, at 359 n.1 (1998), < http://www.verisign.com/respository/baum-ford6-28-99a.doc >.

communicated over open systems such as the Internet, and in particular, are well-suited to support COPA age verification requirements.[5] With few exceptions, only asymmetric cryptography (the technology upon which digital signatures are based) can provide strong support for nonrepudiation.[6]

Digital certificates are highly flexible cryptographic tools, uniquely suitable for satisfying COPA's requirements. For example, digital certificates can be issued to:

> (1) *adults* to authenticate their having attained the age of majority (or any other mandated age), to permit their access to designated web sites and information resources and to exclude children, or
>
> (2) *children* (of any mandated age) to permit their access to designated web sites and information resources, to maintain parental control over children's access, and to exclude adults or other designated classes of persons from specified websites and resources.

In contrast, biometric technologies cannot by themselves secure open, distributed systems (such as the Internet), and PINs/passwords are inherently weak authentication mechanisms. Equally important, digital signatures can protect users' privacy, because (unlike biometrics) they can be communicated without disclosing personally identifiable information from the user.

In any technological system—and particularly one in which security is imperative—certain policy and deployment problems must be resolved if the system is to function properly. The deployment issues surrounding age verification systems for the World Wide Web are reconcilable within the current technological infrastructure of the Internet, if digital signatures and PKI are used as the tools by which age verification is achieved. Therefore we encourage the Commission to advance the use of digital signatures and PKIs as a preferable age verification mechanism for COPA purposes.

[5] The recipient of a digitally signed message may verify the authenticity of the message's digital signature (and thus of the message itself) by applying the signer's public key to the message and digital signature. Only the public key that corresponds to the private key used to sign the message will "match," thereby verifying the authenticity of the digital signature. To do this, the recipient must possess a copy of the signer's public key. One efficient way for a message recipient to obtain a copy of the signer's public key is by obtaining the signer's *digital certificate*. A digital certificate is simply a secured data record that contains the signer's public key, indicates the "binding" (or association) between that public key and the signer, and is itself digitally signed by the issuer of the certificate – a *certification authority* (CA).

[6] Nonrepudiation refers to substantial evidence of (1) the identity of the signer of a message and (2) message integrity, sufficient to prevent a party from successfully denying (i) having originated the message, (ii) that it was delivered, or (iii) the integrity of its contents.

II. Discussion

Public key technology is mature and commercially available

Public key–based technologies have been studied and used by the world's leading mathematicians and cryptographers in academia, industry, and government for many years.[7] For more than a decade, the Department of Defense has been using PKI-based applications to protect the nation's most guarded secrets. Public key–based security has also become ubiquitous in the commercial sector, and is now universally viewed as the predominant enabler of secure e-commerce and communications over the Internet. Governments, banks, universities, and many other users turn to digital certificates for secure e-mail, secure web access to databases, secure data submission via on-line forms, remote dial-up via secure virtual private networks, and many other applications.

To date, VeriSign has issued over 250,000 server certificates, used by web servers for secure and authenticated browser-based communications via SSL; the deployment rate for these certificates is now about 11,000 a month and is increasing by about 20% quarterly. As for individual "client" certificates (similar to those that could be issued to adults or children in satisfaction of COPA), VeriSign has issued nearly 5,000,000 to exchange secure mail, securely access web pages, submit data via secure forms, commute over the Internet to a corporate network, and many other applications.

Furthermore, the commercial PKI industry has established a track record of responding to accelerating demands for on-line security. For example, until recently, organizations wanting to deploy PKIs had to build, operate, and maintain their own PKI systems. The PKI industry responded to this need by making many high-quality security applications available on an outsourced basis, a much simpler and more cost-effective solution.

Two currently available, widespread PKI applications are particularly well suited to COPA's requirements:

[7] For example, the U.S. government has accepted PKI technology as the de facto standard for network security. The Deputy Secretary of Defense has released a policy mandate requiring all DOD users (over 2 million persons) to have a digital certificate by October 2001. Fielding is under way. Many agencies, including the Internal Revenue Service, the Securities and Exchange Commission, the Social Security Administration, and the Department of Veterans Affairs are moving forward with PKI projects. Additionally, the General Services Administration has awarded contracts to commercial certification authorities to issue certificates to citizens for secure on-line access to government benefits-related information and services. See < http://www.ec.fed.gov/aces.htm >. The Government Paperwork Elimination Act (GPEA) provides for federal agencies to give persons who maintain, submit, or disclose information the option of doing so electronically. GPEA requires the use of electronic signature methods, including digital signatures, to verify the identity of the sender and integrity of the associated electronic content.

θ **Secure Web browsing –** Secure Web browsing using the secure sockets layer (SSL) protocol is already an integrated feature of nearly all commercial Web browsers. The SSL protocol relies on digital certificates to provide two-way authentication (the client knows the server to which it is connected, and the server knows the client to which it is connected) and confidentiality for all information communicated between the client and server. These security features are provided without additional effort by the client.

θ **Secure e-mail –** Secure e-mail clients are interoperable using the leading secure messaging protocol (S/MIME). Like the SSL protocol, the S/MIME secure mail protocol is transparent to the users. By simply "clicking" on the desired "sign" and/or "encrypt" icons, the users can both digitally sign and encrypt their mail reliably and conveniently.

Validation of certificate holders

The efficacy of PKI rests largely on the reliability and practicality of the certificate validation process—that is, the process of approving or denying applications for digital certificates based on examination of certain specified credentials. The available validation options are quite broad and provide for great flexibility.

For COPA purposes, authenticating users' age is the key validation issue. The accuracy of the validations produced will depend both on the level of user effort required and on the overall creativity of the validation process. Ultimately there must be a determination of an appropriate level of accuracy to require, weighing the desired level of accuracy against the ease and costs of deployment.

Following are a number of methods for validating user age.[8] Many of these options can be merged to provide potentially stronger and more efficient results. There are theoretically an infinite variety of methods available to complete validation processes as a precondition to certificates deployment. Note that no matter which validation process is selected, it need only be performed *once*, then the validated information (e.g., age) is placed in the digital certificate in a non-forgeable manner such that it can be trusted to be accurate by *relying parties* in an infinite number of subsequent transactions.

θ **Postal Clerks –** This approach is analogous to a postal clerk's current role in validating credentials for a passport. Certificate applicants would present proof of age to a postal clerk. The postal clerk would then examine the documents, query their holder, and either accept or

[8] The order in which these are presented does not reflect any particular preference. Rather, these options are presented simply to demonstrate that significant flexibility exists in validation procedures.

reject the application. Post offices are in close proximity to most citizens, are generally perceived as trustworthy, and produce measurably uniform results.

θ **Notaries Public –** Like postal clerks, notaries are ubiquitous and inexpensive. They provide comparatively strong assurances, since personal appearance of an applicant is required.

θ **Other Trusted Persons –** Other trustworthy persons in a position to identify an individual would include that person's place of work, city clerks, school administrators,[9] and possibly bank trust officers.

θ **Credit Agency or Government Databases –** In this approach, information that is generally unknown to the public is submitted by the applicant online, and the CA checks this information against credit agency or government databases to confirm the applicant's identity.

Biometrics

Biometric identification uses certain biological characteristics (like fingerprints or iris patterns) or behavioral traits (like signature dynamics) of individuals to verify their identity electronically. This technology is in an earlier phase of development than digital signatures and has particular complexities: "[i]n general, biometric identification requires sensors to convert a physical characteristic or behavior . . . into a signal that can be stored, or compared to previously stored signals, using a computer. Consequently, the detailed study of such devices requires the disciplines of human factors, biology, psychology, mathematics, statistics, and electrical and computer engineering."[10] The practical limitations of biometric technologies make them a poor choice to alone support the aims of COPA. Some biometric techniques do possess unique strengths that make them well suited to specific narrow applications, but by themselves they are insufficient to enable secure e-commerce—the strength and breadth of their security features are simply too limited.

[9] For example: After a parent or guardian applies for a digital certificate online on behalf of a child, the certification authority could send follow-up letters to the child's school (as designated in the application) and directly to the parent's home. The letters would contain different PINs. The letter sent to the school would be delivered home by the child, to confirm that the applicant is a parent. (That is, only someone with a child in school would receive such a letter.) The letter sent directly to the parent's home would verify that the applicant is who he or she claims to be. The parent would then enter the two PINs from the two letters into an enrollment form on the CA's web site to obtain the certificate. There are a number of possible variations on this theme that can produce useful results. See < www.cybersmart.org >.

[10] National Biometric Test Center < http://130.65.150.51/faculty/main/nbtc.html >. Dr. Jim Wayman notes that "DNA and all other 'forensic' identification techniques, including latent fingerprint identification, require extensive expert human processing and are not automatic. Therefore, they are not 'biometric identification techniques' according to the definition I use." E-mail from Jim Wayman, director, National Biometric Test Center, to Michael Baum (Nov. 29, 1998) (on file with author).

Moreover, biometric techniques do not themselves solve all the requirements for COPA. Biometric techniques do not lend themselves to readily include validated information (e.g., age) in the biometric signature without using cryptographic mechanisms, like digital signature, to bind them together. Also, biometrics themselves do not provide data integrity and encryption.

PKI offers distinct advantages over biometrics for diverse e-commerce applications, particularly global commerce conducted over the Internet. PKI offers a tested, extensible infrastructure that facilitates commerce conducted over unsecured paths. Therefore biometric technologies are unlikely to achieve the ubiquity of PKI, making them not only impractical but also inconvenient for the purposes demanded by COPA.

The PKI industry and most recognized cryptographers and security experts understand this and have long emphatically embraced the use of biometrics to *supplement and enhance* PKI security, rather than to substitute for it. Thus, biometrics are valuable for controlling local access to computer resources and cryptographic keys contained within a cryptomodule[11]; authorized users can then safely enable digitally signed or encrypted communications over insecure networks or channels, such as the Internet.

Privacy Considerations

It is essential that the technology used to support COPA not compromise an individual's privacy in any way. One cannot extinguish a fire by throwing kerosene on it! Any proposed solution must be closely scrutinized regarding its direct and indirect impact on the individual's privacy. Unlike some other technologies, digital signatures *do not necessarily require users to disclose personally identifiable information when accessing a Web site or other information resource*. They can serve as *age tokens* rather than *identity tokens*. The contrast between digital signatures and biometrics in the area of privacy is particularly stark, since biometrics requires the capture, communication and use of personal data. [12]

[11] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES (1994), *available at* < http://www.itl.nist.gov/div897/pubs/fip140-1.htm >.

[12] Also, "[b]iometric authentication technologies have limitations when employed in network contexts because the compromise of the digital version of someone's biometric data could allow an attacker to impersonate a legitimate user over the network." FRED B. SCHNEIDER, ED., COMMITTEE ON INFORMATION SYSTEMS TRUSTWORTHINESS, COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, COMMISSION ON PHYSICAL SCIENCES, MATHEMATICS, AND APPLICATIONS, NATIONAL RESEARCH COUNCIL, TRUST IN CYBERSPACE, at ch. 7 (1998), < http://cryptome.org/tic.htm >.

Industry Self-regulation

With the recent acceleration and adoption of PKIs in both the public and private sectors, and perhaps with some modest encouragement from the Commission, the adoption of PKIs by Web sites and other information resource entities to assure the protection of children is promising. As the Commission becomes more familiar with the demonstrated capabilities of PKI, it can fashion proposed solutions that are less-burdensome and onerous to both the protected classes under COPA as well as to the industries that can enable such solutions. Consequently, it is urged that any proposed regulation be incremental and sensitive to the positive impact of commercial PKIs on available solutions. VeriSign is pleased to work with the Commission to further elaborate an appropriate solution that exploits the benefits of PKI.

About VeriSign

Information about VeriSign, digital signatures, and public key infrastructures is available at < http://www.verisign.com >.

***