



The National Electronic Commerce
Coordinating Council

*Hey! Where Did the Good Ole
'Dotted Line' Go?*

Prepared by the Lessons Learned: E-Signatures Statutes Work Group

Presented at the NECCC Annual Conference, December 4-6, 2002, New York, NY

NATIONAL ELECTRONIC COMMERCE COORDINATING COUNCIL

In 1997, as the use of the Internet was increasing at a stunning rate, a group of public and private professionals—government executives and information technology practitioners—met in San Antonio, Texas to discuss their common issues, problems and ideas. This first meeting was productive. Participants learned from each other. They felt that continuing to meet as a group would help them meet the challenges and opportunities posed by the rush of engulfing information technologies. This founding group formed the National Electronic Commerce Coordinating Council (NECCC), which has continued to meet regularly.

Today, NECCC serves as an alliance of government organizations dedicated to promoting electronic government through the exploration of emerging issues and best practices. Alliance partners are the National Association of State Auditors, Comptrollers and Treasurers; the National Association of Secretaries of State NASS; and the National Institute of Governmental Purchasing.

NECCC also works in partnership with these affiliate organizations: the Information Technology Association of America; National Automated Clearing House Association; National Association of Government Archives and Records Administrators; and National Association of State Treasurers

CONTACT INFORMATION

The National Electronic Commerce Coordinating Council
2401 Regency Road, Suite 302
Lexington, KY 40503
P: (859) 276-1147
F: (859) 278-0507
www.ec3.org

2002 NECCC EXECUTIVE BOARD

Signatory Members

Chair, *J. Kenneth Blackwell*, NASS, Secretary of State, Ohio
Vice Chair, *Ralph Campbell, Jr.*, NASACT, State Auditor, North Carolina
Secretary/Treasurer, *Mary Kiffmeyer*, NASS, Secretary of State, Minnesota

Steve Adams, NASACT, State Treasurer, Tennessee
David Dise, NIGP, Procurement Manager, Fairfax County Water Authority, Virginia
Rick Grimm, NIGP, NIGP Chief Executive Officer, Virginia
Stephen Gordon, NIGP, Purchasing Agent, Metropolitan Govt. of Nashville/Davidson County, Tennessee
Elaine Marshall, NASS, Secretary of State, North Carolina
Robert Childree, NASACT, State Comptroller, Alabama

Affiliate Members

P.K. Agarwal, ITAA, CIO and Executive Vice President, National Information Consortium
William Kilmartin, NACHA, Vice President, Accenture
Jack Markell, NAST, State Treasurer, Delaware
Amelia Winstead, NAGARA, State and Local Government Services Manager, Office of the Secretary of State, Georgia

Ex-Officio Members

Carolyn Purcell, CIO, Department of Information Resources, Texas
Basil Nikas, CEO, iNetPurchasing
J.D. Williams, Director, State and Local Government, PeopleSoft, USA, Inc.

At-Large Members

Avi Duvdevani, CIO/Deputy General Manager, New York
Daniel Greenwood, Director, MIT E-Commerce Architecture Program, Massachusetts Institute of Technology
David Lewis, Retired Director and CIO, Massachusetts
Jay Maxwell, Senior Vice President, AAMVA
Eric Reeves, State Senator, North Carolina
David Temoshok, PKI Program Manager, Government Services Administration
Costis Toregas, CEO, Public Technology, Inc.
Susan Hogg, Chief, Statewide e-Government Initiatives Office

TABLE OF CONTENTS

I.	Introduction.....	1
II.	E-Signature Statutes.....	1
	a. The Laws	
	i. Electronic Signatures in Global and National Commerce Act, “E-SIGN”	
	ii. Uniform Electronic Transactions Act, UETA	
	b. Electronic vs. Digital Signatures	
	i. Electronic Record and Electronic Signature Defined	
	ii. Digital Signature Defined	
III.	E-Signature Trends for 2003.....	6
	a. Overview of Legal Trends	
	i. New Federal and State Legislation	
	ii. State Implementation of UETA and E-SIGN	
	iii. Will More States Pass e-Signature laws?	
	b. Government Trends	
IV.	Current Uses of Electronic Contracting by Government Agencies.....	12
	a. Interview #1: <i>Paula Arcioni, PKI Directory Services and Identity Management manager, state of New Jersey Department of Labor</i>	
	b. Interview #2: <i>Jim Samual, Chief of Corporate Affairs, Ohio Bureau of Workers’ Compensation</i>	
	c. Interview #3: <i>Tamee Roberts, State of Utah, Department of Community and Economic Development</i>	
V.	Conclusion.....	17
	Appendix A.....	18
	I. Legal Trends	
	a. Court challenges and questions of how certain terms in E-SIGN law applies to government	
	i. Although E-SIGN and UETA have not been test in court, judges routinely enforce electronic contracts based on basic contract principles	
	ii. E-SIGN may face judicial scrutiny in public procurements	

Electronic Signature Statutes

I. Introduction

When this project was started back in April, the first question on everyone's mind was "What *have* we learned in the realm of E-Signature Statutes?" Looking back at the history and legislative activity surrounding UETA and the many state statutes is a necessary level of inquiry, *yet where are we in regards to moving forward and setting precedent and good practices for the future in this ever-evolving topic?* Because of the speed of technology evolution, advanced systems can become outdated in as short as two years, and the electronic signature statute of today is quite malleable in terms of its application in the future.

Signing on the "good ole' dotted-line" is quietly being replaced in several different areas with the modern e-signature transformation. This paper represents the work of one of three subgroups within the "Lessons Learned" Workgroup of the 2002 National Electronic Commerce Coordinating Council (NECCC). What you are about to read contains some of the success stories from across the country in the domain of electronic signatures. States such as Utah, Ohio and New Jersey have attempted to streamline and reduce the costs associated with doing business on an everyday basis, with e-signature advancements representing a key component of those savings.

In addition, this paper will take you through the very beginnings of the electronic signature revolution, noting such key pieces of legislation as the Electronic Signatures in Global and National Commerce Act (E-SIGN) and the Uniform Electronic Transactions Act (UETA). It will also give the most up-to-date trends in digital signature e-government applications, as well as legal trends in the validity of what constitutes a true, binding electronic signature when used in a contract.

II. E-Signature Statutes

a. The Laws

The purpose of the Electronic Signatures in Global and National Commerce Act (E-SIGN) and the Uniform Electronic Transactions Act (UETA) is to validate the use of electronic signatures, electronic records and electronic contracting agents. The goal of these laws is to facilitate electronic commerce, not to replace existing laws. Neither law requires the use of electronic signatures nor establishes technology requirements for electronic transactions.

i. *Electronic Signatures in Global and National Commerce Act, "E-SIGN"*

E-SIGN was signed by President Clinton on June 30, 2000 and became effective on October 1, 2000. E-SIGN is a federal law that validates the use of electronic signatures, electronic records and electronic agents.

The scope of E-SIGN is wide as it applies to electronic contracts and signatures on records used in “any transaction in or affecting interstate or foreign commerce.”¹ “Transaction” is broadly defined to include any action “relating to the conduct of business, consumer, or commercial affairs” between two or more “persons.”² E-SIGN applies to the sale, lease, licensing or other disposition of personal property (including goods and intangibles), services or real property.³ Government agencies are included in the definition of “persons” in the Act.⁴

E-SIGN does not apply to legal instruments involving personal matters (such as wills, codicils, or testamentary trusts, adoption, divorce, or other family law matters), consumer protection notices involving utility service termination, possession of an individual’s primary residence, health or life insurance termination, or product recall or failure; and public safety issues, such as documents required to accompany transportation of hazardous, toxic, or dangerous materials. E-SIGN also does not apply to court orders, notices, or documents, or to transactions governed by the Uniform Commercial Code, with certain exceptions.

E-SIGN does not preempt the effect of any other legislation or regulations relating to limitations on the legal effect or enforceability of contracts, records, and signatures, *except* to the extent that a regulation or law requires paper writing.⁵ E-SIGN also does not limit or supersede any requirement relating to the standards or formats for records filed with federal or state regulatory agencies.⁶ Finally, E-SIGN does not preempt or preclude state law or regulation relating to electronic records or signatures so long as the law or regulation is consistent with or is an enactment of UETA.⁷

The E-SIGN statute includes consumer protection provisions that require the consumer to “opt-in” by affirmatively electing to enter into an electronic contract. These requirements include:

- Affirmative consent by the consumer after having the opportunity to review a clear and conspicuous statement of their rights, the scope of their consent and how to withdraw consent;
- informing the consumer of the hardware and software requirements for accessing and retaining the electronic records; and

¹ 15 U.S.C. § 7001(a).

² 15 U.S.C. § 7006(13).

³ 15 U.S.C. § 7006(13).

⁴ 15 U.S.C. § 7006(8).

⁵ 15 U.S.C. § 70001(b)(1).

⁶ 15 U.S.C. § 7004(a).

⁷ 15 U.S.C. § 7002(a).

- electronic confirmation by the consumer that demonstrates their ability to access information in the electronic format that will be used to provide the information that is the subject of their consent.

E-SIGN specifically permits for retention of contracts and records in an electronic format in §101(d), “Retention of Contract and Records”. Where a statute, regulation or other rule of law requires retention of a record or contract, E-SIGN establishes that the requirement may be met by retaining an electronic record of the information contained in the contract or other record. For the electronic record to be valid, E-SIGN requires that the electronic record accurately reflect the information contained in the contract or record and remain accessible by all persons who are entitled to access.

ii. Uniform Electronic Transactions Act – “UETA”

The National Conference of Commissioners of Uniform State Laws approved and recommended UETA for adoption by the states in July 1999. UETA is a model state law that preempts E-SIGN when adopted without substantial modification by a state. UETA is very similar to E-SIGN in its intent to facilitate electronic commerce by validating the use of electronic signatures and records. UETA is not intended to modify current laws. “It is important to understand that the purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures. According to a 1999 UETA prefatory note, it is not a general contracting statute - the substantive rules of contracts remain unaffected by UETA. Nor is it a digital signature statute. To the extent that a State has a digital signature law, the UETA is designed to support and compliment that statute.”

UETA applies to electronic records and electronic signatures relating to a transaction. Similar to E-SIGN, UETA does not apply to transactions governed by laws related to the creation and execution of wills, codicils or trusts, any articles of the Uniform Commercial Code other than Articles 2 and 2A. And, like E-SIGN, UETA validates the retention of records in an electronic format.

b. Electronic vs. Digital Signatures

i. Electronic Record and Electronic Signature Defined⁸

E-SIGN’s definition of “electronic record” is broadly drafted to cover almost any form of electronic communication. Contracts, records and related communications that are transmitted or stored in e-mail, the Internet, diskette, compact disk, or other similar form all fall within the ambit of E-SIGN.⁹

The definition of “electronic signature” is important because it establishes the requirements for making an electronic record enforceable. The statute defines “electronic

⁸ This section is excerpted from “The “E-Sign” Law: What Does it Mean for Government Contracting Practices?”, NCMA World Congress, July 23, 2002 written by Allen Samelson and Anthony Bedwell-Coll.

⁹ 15 U.S.C. § 7006(9) (defining “record” as “information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form”).

signature” as “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”¹⁰ Thus, for the purpose of contract enforcement, the two critical requirements are that an electronic sound, symbol, or process must be (1) “associated with” a contract or other record, and (2) adopted by the signatory with the intent to sign the record. These requirements can be difficult to prove in the transitory world of electronic commerce. It is significant, however, that under E-SIGN any symbol or process can qualify as an electronic signature, as long as it is properly connected with the contract and shown to have been made (or later adopted) by a person having the intent to sign it.

In this sense, E-SIGN adopts an age-old rule from the common law of contracts: any symbol that the sender intends to serve as a signature will suffice, irrespective of the technology used to do so -- a name on a telegram communicated orally to an operator, a telex transmission, a handwritten or typed fax, a printed name and logo on a pre-printed form,¹¹ or, indeed, even a pencil.¹²

A variety of processes can be used to indicate through an electronic medium that the signing party has in fact assented to the message received. Electronic signature processes can range in complexity from the sending of a simple e-mail to the use of encryption technology.¹³ The development of more sophisticated signature processes has been spurred by the desire to ensure compliance with the two elements of the contracting process captured in the E-SIGN electronic signature definition noted above.

¹⁰ 15 U.S.C. § 7006(5).

¹¹ See Suzanne Sherry, “Haste Makes Waste: Congress and the Common Law in Cyberspace,” 55 Vand.L. Rev. 309, 358-359, n. 182-185 (March 2002).

¹² In the 1817 decision in *Executors of Claron v. Bailey*, 14 Johns. 484 (N.Y. 1817), 1817 N.Y. LEXIS 136, the New York Court for the Correction of Errors upheld a pencil-signed contract, asking “What have we to do with the kind of instrument which the parties employed? . . .” See, Note: *The E-SIGN Act of 2000: Triumph of Function over Form in American Contract Law*, 76 Notre Dame L. Rev. 1183, 1190, n. 29-32 (2001).

¹³ Because this is a developing area of the law, many terms describing electronic signatures have been used in different ways by legislatures and commentators. The following definitions are given to these terms, as used in this article:

- (1) Electronic Signature: any sound, symbol, or process using an electronic medium to identify an individual (i.e., a password, an email, or any of the other forms of electronic signature identified below).
- (2) Digital Signature: an electronic signature using asymmetric cryptography to encrypt and decrypt messages (explained more fully further later in this article).
- (3) Digitized Signature: a digital image of a physical signature created either by scanning a physical signature or by using stylus, sensing pad, or similar device (even a mouse) to create a digitally replicated signature.
- (4) Biometric Signature: an electronic signature incorporating some element of personal physiology, such as a voice imprint, a retinal scan, or a hand scan. One Biometric Signature that is commercially available and authorized by the California Secretary of State for use in public procurement is called Signature Dynamics, which uses a stylus and pad to measure the pressure and speed of an individual’s signature to identify the signing party.

ii. Digital Signature Defined¹⁴

A digital signature links a person's identity to a specially encrypted private key that is issued to only one bearer. The private key can be used to electronically sign a communication, which can then be opened by someone with the public key. A certificate authority maintains the public key and also issues and verifies the digital certificates that validate the identity of each party in an Internet transaction. The basic element of any public-key infrastructure is the digital certificate. Like a driver's license entitles its holder to navigate the roads, a digital certificate lets its holder navigate a secure network.

Digital signatures, like their written counterparts, are able to identify the sender by linking the authenticated document back to the signor. By going through the motions of digitally signing, the sender formalizes the agreement, evidences his approval of the agreement, and signals the legal significance of electronically signing. The signatures also protect the documents, which become difficult to alter by third parties that may intercept the digitally signed document.

Because messages on the Internet are not sent over a single pathway, but are transmitted over a series of thousands of networks, a message must move from network hub to the next network hub on the Internet before reaching its final destination. The result is that any person with access to any intermediate hub, can intercept, read, or alter an electronic message in a way that is undetectable by the recipient. With the passage of a digital signature act or its equivalent, states have a mechanism for protecting and enforcing digitally signed contracts.

A digital signature is *not* a scanned replica of a handwritten signature. A digital signature consists of an encrypted or mathematically scrambled document with a string of characters appended to the message that serve to identify the sender and the integrity of the document. Only someone with the proper software can decode the message. Digital signatures are typically generated using a public key (PKI, as discussed earlier in this chapter), or an asymmetric cryptosystem. Asymmetric cryptosystem is based on the use of two software codes, or public/private key pair, to send and receive documents. The "private" key is kept secret by its owner and is used to encode the text of a document into the digital signature. The "public" key is made publicly available to persons who may be dealing with the owner or sender of the document and who need to decode the transmission. The "public" and "private" keys are mathematically related, but the relationship is so complicated that it is "computationally infeasible" to deduce one key solely from knowledge of the other key. The keys are such that the other key can only decrypt the digital signature created by one key. Hence, when used in conjunction with one another, the public/private key system provides complete security.

The major problem with the public/private key system is verifying that the sender of the document is who they say they are. The recipient can verify that the message is

¹⁴ This section is excerpted from Chapter 4 of Legal Aspects of Purchasing, written by Kirk Buffington, to be published by the National Institute of Governmental Purchasing in 2003. Copyright NIGP. Used by permission.

from the sender by verifying the signature with the sender's public key, but if key pairs are not licensed to any specific individual, the recipient has no way of verifying the actual identity of the sender. If you cannot relate the public key to a real person you can trust, you still cannot trust the document. This is analogous to the situation where you have received a properly signed check but still cannot tell whether or not the check is good, because you do not know what the account holder's signature looks like. This is the reason a digital signature should be notarized. According to the American Bar Association's guidelines on digital signatures, "Some convincing strategy is necessary to reliably associate a particular person or entity of the key pair."

The licensed CAs performs substantially the same function as a notary would for written documents, except now that role has exploded as business transactions have moved to the Internet to take advantage of its efficiencies. Generally, a digital signature notarization service issues a digital certificate that ties the registered private/public key pair with the identity information of its owner. The digital certificate is signed by the issuer's digital signature and can be verified using the issuer's public key, which is usually well publicized. This certificate is made publicly available in a "repository" maintained by the CA or someone else. A recipient of a digitally signed message will access the certificate and determine that a public key is associated with a private key possessed by a certain person, obtain a copy of that public key, and then use that public key to decrypt the digitally signed message the recipient (i.e., vendor) has received. After verifying both the signature on the message and the certificate notarizing the signature, the party is ensured that the message is truly from the person identified by the information included in the notary certificate.

In addition to being a reliable method of identifying the source of an electronic message, a digital signature is also very good evidence that the message has not been tampered with since transmission. Any alteration of a digitally signed message will cause the public key to fail to decipher the digital signature, thus indicating to the recipient that the message has been tampered with since it was digitally signed. Hence, assuming that the CA has effectively verified the identity of the person associated with the public key, and assuming that person has exercised reasonable care to prevent the loss or compromise of the private key, the use of digitally signed documents provides an extraordinarily reliable method of validating both the source and the content of an electronic transmission.

III. E-Signature Trends for 2003

a. Overview of Legal Trends

For a detailed survey of the legal trends and recent court decisions, please see Appendix A, "Legal Trends"

Most states have passed some form of electronic signature legislation. Most states have already adopted some form of UETA, and those states that previously passed technology specific legislation, such as laws that only recognize the validity of digital signatures, are currently bringing their laws in line with the technology neutral

framework of UETA and E-SIGN. Nonetheless, many states continue to have technology preference laws in place, including laws that mandate technology specific electronic signature methods for certain types of transactions, such as transactions with government agencies.

On the federal level, the most active legislation at this time is the federal E-Government Act of 2002. The Act creates a new Office of Electronic Government within the OMB, mandates the creation of an Chief Information Officers Council that will coordinate efforts for e-government initiatives, and appropriates over \$350 million dollars for various electronic government initiatives over the next four years.

Although recently enacted electronic signature laws have not yet been interpreted by the courts, the validity of electronic contracts has been firmly established under basic contract law principles. Many courts have upheld the validity of “click-wrap agreements” (e.g., electronic software licenses accepted by clicking an “I accept” button), so long as the person accepting the goods or services is required to access the terms and conditions before clicking on an acceptance icon. Moreover, several courts have enforced contracts where email exchanges provide evidence that the parties have reached an agreement to which they intended to be bound.

A likely setting in which E-SIGN might be challenged in court in the future is in the area of public contacting. Arguably, E-SIGN requires public agencies to use and accept electronic signatures when they engage in commercial transactions subject to the statute. However, the federal Office of Management and Budget (“OMB”) has issued guidance, which states that E-SIGN does not require public agencies to use electronic signatures, despite statutory language specifically targeting the use of electronic signatures by public agencies in such circumstances, other than in the contracts themselves.

i. New federal and state legislation

On May 1, 2001, Senator Joseph Lieberman introduced Senate Bill 803, known by its short title as the “E-Government Act of 2002” (“E-Gov Act”). If enacted, the E-Gov Act will likely result in an increasing drive toward widespread use of electronic records and signatures by federal agencies. The E-Gov Act will establish an Office of Electronic Government within the Office of Management and Budget (“OMB”), which will work with the OMB director and other agency heads in establishing standards for the use and interoperability of electronic records and signatures among federal agencies.

The E-Gov Act also requires each executive agency to “ensure that its methods for use and acceptance of electronic signatures are compatible with” the policies and procedures to be established by the director of OMB. Section 203 of the Act charges the administrator of general services with assisting the OMB director “by establishing a framework to allow efficient interoperability among executive agencies when using electronic signatures, including processing of digital signatures.”

The E-Gov Act is not merely directive; it also provides funding to implement its goals. Section 203 authorizes an \$8 million appropriation for fiscal year 2003, “and such sums as are necessary” for subsequent years, for development of a federal digital signature compatibility bridge. The Act also establishes an E-Government Fund to support agency projects approved by the OMB director that are intended to develop and implement federal agencies’ use of information technology. The Act appropriates a total of \$345 million for fiscal years 2003 through 2006 for the fund and “such sums as are necessary” for fiscal year 2007.

Additionally, the Act will establish a Chief Information Officers Council, which will include, among others, the deputy director for management of the OMB, the administrator of the Office of Electronic Government, and the CIOs of the Central Intelligence Agency and the departments of the Army, Navy, and Air Force. Under proposed section 3603(f), the CIOs Council will be responsible for developing recommendations to improve the development and use of information technology resources among federal agencies.

The Senate passed the E-Government Act of 2002 on June 27, 2002. A House version of the Act was introduced on July 11, 2001 and is being considered by the House Committee on Government Reform, along with the Senate’s engrossed bill. As of November, 2002, the Bush administration has indicated its support of the Act.¹⁵

ii. State Implementation of UETA and E-SIGN¹⁶

State statutes relating to electronic signatures and contracts may be grouped into three broad categories:

- a) Technology Neutral laws: A majority of states with electronic records and signature laws have adopted UETA wholesale or in substantial part. These States allow any form of electronic signature to be binding so long as the parties have agreed to the use and type of signature and the signing party intended to be bound by the signature. In those states no specific signature technology is given prominence over other technologies.¹⁷
- b) Technology Preferred laws: Some states have adopted laws that appear to be technology neutral, but provide an evidentiary presumption in favor of validity if the parties use specific technologies. Although a specific technology may not always be expressly identified, in order to be

¹⁵ “Administration Supports Revised Version of Lieberman Bill Passed by Senate,” 78 Federal Contracts Reports 335, 345 (September 24, 2002).

¹⁶ This section is excerpted from “The “E-Sign” Law: What Does it Mean for Government Contracting Practices?”, NCMA World Congress, July 23, 2002 written by Allen Samelson and Anthony Bedwell-Coll.

¹⁷ See, e.g., Idaho Code §§ 28-50-101 et seq.; Kan. Stat. Anno. §§96-601 et seq.; Mich. Comp. Laws §§ 450.834 et seq.; and Tex. Bus. & Prof. Code §§ 43.001 et seq.

eligible for the presumption, the “secure electronic signatures” must meet specified criteria, which only certain technology (typically, digital signatures) may satisfy.¹⁸

- c) Technology Specific laws (the “Utah Model”): Under the law of some states, only specifically identified technologies, usually digital signatures, can be used in order to have a valid electronic signature. Utah was the first state to pass such an electronic signature law.¹⁹ Other states subsequently adopted digital signature specific statutes²⁰ or statutes, like those containing presumptions for “secure electronic signatures,” that require specific criteria to be met for the signature to be deemed valid. Thus far, only Digital Signatures or signatures using Signature Dynamics technology have been identified as acceptable under such statutes.²¹

Many states have passed more than one statute relating to electronic signatures. For example, after Utah passed the first electronic signature statute, which specified digital signatures only, its Legislature later enacted UETA on March 7, 2000.²² Additionally, some states have passed UETA, which applies to all transactions, as well as more restrictive laws for specified transactions (typically involving government agencies).²³ This mosaic of electronic signature laws requires careful analysis to determine not only whether a state has passed an electronic signature law(s), but also which one applies to the transaction at issue. As of October 2002, UETA has been enacted in some form in thirty-nine states, as well as the District of Columbia, and is pending in six more states. Alaska, Georgia, New York, and Washington remain in the small minority, as those states have not adopted any form of UETA and they do not have an UETA initiative pending.

The New York Attorney General recently considered whether E-SIGN preempts New York’s law governing recordation of real property transfers. The Attorney General concluded that there is a substantial possibility that E-SIGN does not pre-empt New York’s recordation law based on the statute’s exception for laws regulating purely governmental activities. *Id.* at *18.

¹⁸ See, e.g., Ariz. Rev. Stat. § 44-7031; Ill. Comp. Stat. §§ 5 ILCS 175/10-110 et seq.; and Wash. Rev. Code § 19.34.360. In order for an electronic signature to be considered a “secure electronic signature,” it usually must be: “(1) Unique to the person using it; (2) capable of verification; (3) under the sole control of the person using it; and (4) linked to the electronic record to which it relates in such a manner that if the record were changed the electronic signature would be invalidated.” Ariz. Rev. Stat. § 44-7031. The second and fourth criteria effectively eliminate all technologies other than Digital Signatures (and Signature Dynamics) because they include security measures (certificate authorities) which control access to the electronic signature and record.

¹⁹ Utah Code Anno. §§ 46-3-101 et seq.

²⁰ See, e.g., Mo. Rev. Stat. § 26.600 et seq.

²¹ See, e.g., Cal. Gov. Code § 16.5; N.Y. CLS St. Tech. Law §§ 101 et seq.

²² See Utah Rev. Stat. § 46-4-101.

²³ See, e.g., Cal. Gov. Code § 16.5 (requiring transactions with government agencies using electronic signatures to be conducted using technologies approved by the Secretary of State).

iii. Will more States pass e-Signature laws?

As indicated, the vast majority of states have adopted some form of UETA. As of November, 2002, very few States have e-signature laws pending and the few active bills either recently passed or presently being considered are amendments to prior laws, which have been introduced in order to bring a state's electronic signature laws in line with E-SIGN and UETA.

For example, the Legislature of New York, one of the first states to pass a digital signature law, recently passed an amendment to ESRA that fundamentally changed its definition of "electronic signature." Prior to the amendment, ESRA's electronic signature definition was limited to an electronic identifier that met specified criteria, including a requirement that the identifier was "attached to or associated with data in such a manner that authenticates the attachment of the signature to particular data and the integrity of the data transmitted," (i.e., a digital signature). In order to "ensure that [ESRA and E-SIGN] continue to complement each other in achieving" expansion of electronic commerce, the New York Legislature passed, and on August 8, 2002, the Governor of New York signed into law, an amendment to ESRA that changed the definition of "electronic signature" to "an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record."

Illinois is presently considering a bill to amend its Electronic Commerce Security Act. Finally, on September 13, 2002, the Governor of California signed into law amendments to California's version of UETA, which had been widely criticized for its prior non-uniform enactment.

b. Government Trends²⁴

To appreciate the push for increased adoption of e-procurement, an understanding of the whole movement towards e-government in general is appropriate. In the 1970s, the idea that every secretary would be outfitted with a computer at his or her workstation was far-fetched and seemed futuristic.²⁵ Today, even those working outside the office have access to computers, and frequently use them to carry out their duties more effectively and efficiently.

Online government services have also increased, and as North Carolina's Chief Information Officer, Ronald P. Hawley, puts it, "people expect government services to be

²⁴ This section excerpted from Kirk Buffington's article, "Supplier Enablement and Engagement: eprocurement".

²⁵ Barrett, Katherine, and Richard Greene. 2001. *Powering Up: How Public Managers Can Take Control of Information Technology*. Washington, D.C.: CQ Press.

on line”.²⁶ While some state and local governments were slow in embracing web-based technology in the early 1990s, other governments like the state of Washington were pioneering its use. Some of the early pioneers in Internet technology can be identified by their e-mail suffix. The e-mail suffix “.gov” now belongs to the federal government exclusively, but some states and local governments like the state of Washington still use “.gov” at the end of their e-mail addresses because they were among those governmental entities that adopted the technology early and were grand-fathered in for the use of that suffix.²⁷

The Internet has been put to some innovative uses by government. In early 2001, the state of Michigan was exploring the possibility of establishing a cyber-court in which specially trained judges would interact with lawyers and witnesses via the Internet.²⁸ At that time nine states, which include California, Delaware, Illinois, Maine, Maryland, Massachusetts, Minnesota, New Mexico, and New York, had already afforded taxpayers the option of filing personal income at their Web sites.²⁹ The state of Missouri issues electronic benefits transfer cards to recipients of welfare benefits, which has reduced paper work and the need for printing checks and food stamps. The cards may be used at ATM machines to access unemployment money and make payments to vendors for items under the food stamp program. Qualified recipients can use their cards to make payments in the same manner a bank debit card works.³⁰ The Tulsa Fire Department in Oklahoma is one of the governmental organizations that now use video streaming technology to train firefighters without them having to leave their posts.³¹ Prior to the installation of the system, the Fire Department had to offer the same classes several times to different groups of fire fighters.

Many state governments have invested much in equipment to give increased access to their citizenry. Oregon’s Employment Department placed more than a hundred kiosks with touch-screen capability around the state, and provides job listings and other information to the public.³² Police departments around the nation now have law enforcement officers using wireless applications to run criminal background checks on suspects in the field, without having to wait on someone at the station to access and then forward the information. The Alexandria Police Department is one of those departments that now have the capability to digitally transmit images of suspects and missing persons to officers equipped with mobile pocket computer technology. Like others around the

²⁶ Young, Donna. 2001. “E-filing saves time, money.” *Government Computer News / State and Local*. Vol 7, No. 4. April 2001.

²⁷ Barrett, Katherine, and Richard Greene. 2001. *Powering Up: How Public Managers Can Take Control of Information Technology*. Washington, D.C.: CQ Press.

²⁸ Conradi, Melissa. 2001. “Grabbing the E-Gavel.” *Governing: The Magazine of States and Localities*. Vol. 14, No. 8. May 2001.

²⁹ Young, Donna. 2001. “E-filing saves time, money.” *Government Computer News / State and Local*. Vol 7, No. 4. April 2001.

³⁰ Barrett, Katherine, and Richard Greene. 2001. *Powering Up: How Public Managers Can Take Control of Information Technology*. Washington, D.C.: CQ Press.

³¹ Wade, Beth. 2001. “Tulsa Offers Distance Learning to Firefighters.” *American City & County*. Vol. 116, No. 7. May 2001.

³² Barrett, Katherine, and Richard Greene. 2001. *Powering Up: How Public Managers Can Take Control of Information Technology*. Washington, D.C.: CQ Press.

country, the department also conducts its roll call via computers, a practice that saves time and reduces paperwork. Because of the pace of its evolution, most of the technology discussed in this paper may become basic in another year or two, or replaced by more advanced systems. As known, it was barely a decade ago when fax machines were the newest hot technology in offices.³³

The federal government is actively pursuing e-government in general and e-procurement in particular. After all, the federal government took the forefront in the movement to aggressively develop the Internet. In early 2001, Senator Joe Lieberman teamed up with Senator Conrad Burns to introduce the e-Government Act of 2001, in what Sandra Wimmer describes as “an effort to maximize the quality of the federal government’s online resources, as well as reduce overall costs”.³⁴ The Act is co-sponsored by several other prominent senators, including John McCain, Thomas Daschle, John Kerry, Patrick Leahy, and others. The Act, among other things, seeks to establish a federal Chief Information Officer (CIO), authorize \$200 million a year for an e-government fund, establish an online directory of websites, institute an online national library, and fund a federal training center for IT professionals.

IV. Current Uses of Electronic Contracting by Government Agencies

Various government agencies were interviewed to identify and assess electronic contracting activities and the role of e-signature legislation. The following represents the results of those interviews and is intended to provide examples of current electronic contracting initiatives.

a. Interview #1: Paula Arcioni, PKI Directory Services and Identity Management manager, State of New Jersey Department of Labor³⁵

After a successful pilot project in 2002, the New Jersey Department of Labor launched a PKI application for a program that will allow employers in the state to apply for grant funds for workforce training. According to Paula Arcioni, head of PKI directory services and identity management, the program requires “non-refutable formal contracts” that include signature authentication of multiple participants including employers, representatives of the state’s Department of Labor, agency chiefs and chief financial officers.

Because these contracts will be shared electronically with numerous parties, just as they are in the paper-based world, the department needed to ensure the authenticity of

³³ Barrett, Katherine, and Richard Greene. 2001. *Powering Up: How Public Managers Can Take Control of Information Technology*. Washington, D.C.: CQ Press.

³⁴ Wimmer, Sandra. 2001. “Parties Partner; Public to Profit”. *Government Procurement: The Journal of the Purchasing Professional*. Vol. 9, No. 2. April 2001.

³⁵ Darby Patterson interviewed Paula Arcioni PKI Directory Services and Identity Management manager, state of New Jersey Department of Labor. paula.arcioni@oit.state.nj.us

signatures that would be legally enforceable. In signing the papers, employers agree to provide specific training to participants and adhere to “the letter of the law,” according to Arcioni.

The New Jersey Legislature passed the Uniform Electronic Transactions Act (UETA) in 2001. But, prior to that, PKI had been used in a pilot project for the Work Force Investment Act that linked the departments of labor, human services and health. The state’s Bureau of Workers’ Compensation also did an authentication project using PKI. The project later received an award from the National Association of State CIO’s.

These early PKI implementations convinced state IT officials that PKI could be leveraged across the enterprise. Arcioni said the DOL is “fairly innovative in their use of PKI technology” and quickly recognized its potential to streamline the DOL’s work force training initiative – the kind of project that is traditionally awash in paperwork.

The cost of rolling out approximately 500 PKI signatures fell within the department’s planned budget with one exception. According to Arcioni, the department had not anticipated the need to purchase a Certificate Policy Document and a Certificate Practices Statement document – both are required for PKI legitimacy.

The state serves as its own certificate authority, using Versign for facilities management. There are three levels of authentication, reflecting high, medium and low levels of trust. The first requires that an individual is identified in person by physical presence; the second depends on the individual being identified through some remote means such as in the context of a “trusted business partner” and third and least secure, is identity via email. Arcioni says this lowest level is seldom used.

The greatest challenge in implementing the grant program was getting participants to understand the value and operational details of PKI. Arcioni called the technology “arcane and complicated.” Even some technologists, she said, seemed to resist the concept. She found herself spending inordinate amounts of time simply explaining how PKI works and why it is necessary for certain online transactions. On the other hand, the usefulness of the technology sold itself in small project that involved tape submission and data entry. PKI served as an authentication tool to help automate a mostly manual process. Arcioni says she is looking for other opportunities to test this application of PKI.

A continuing frustration, according to Arcioni, is the slowness with which PKI is being implemented. One reason for this, she speculates, is that many software development kits are cost prohibitive for governments. Instead of being expensive and difficult to use, Arcioni says that vendors would be better served by making it easier to develop and use the technology so that smart cards, key fobs and nonreputable signatures become common tools in government operations. But, like many issues in e-government, Arcioni says it’s really not the technology that’s challenging. “PKI is 15 percent technology,” she said, “and maybe 65 percent legal and the rest is policy and business.”

With a better understanding of PKI and successful projects in operation, Arcioni anticipates extending the benefits of e-signatures to local governments. Suggesting that local governments might serve as the registration authority, she said the legal issues surrounding PKI are the same, regardless of jurisdiction. To date, governments have been mostly picking “the low hanging fruit” of PKI and its potential is yet to be tapped, she added.

b. Interview #2: Jim Samual, Chief of Corporate Affairs, Ohio Bureau of Workers’ Compensation³⁶

The Ohio Bureau of Workers’ Compensation launched its interactive Web site, Dolphin, in October of 2000. By April of the following year, the site had over 30 services and more than 90 features. With more than 50,000 online accounts, Dolphin won the 2002 Ohio E-Commerce Award for innovation in the government sector. The site averages 15,000 visits per day. Registered users are equipped with digital signatures that enable more than 1,000 daily transactions.

Dolphin allows injured workers to file online claims, manage their accounts and communicate with bureau personnel. Authorized lawyers and physicians can also access files. Recently, the bureau launched a pilot project that permits doctors to review cases online. Access to all these services requires the issuance of a digital signature.

In crafting legislation to enable the use of digital signatures, the bureau had some influential assistance. Representatives from both houses of the state legislature were members of the BWC oversight commission and clearly understood the importance of digital signature legislation in moving the ambitious project forward. In addition, the department had the support of Gov. Bob Taft who spoke on behalf of the proposed bill. Within months the bill passed the legislature and was on the governor’s desk.

According to Jim Samuel, BWC’s chief of corporate affairs, the legislation also “cleaned up” some old language that no longer applied to the Information Age. References to specific technologies were omitted in favor of the more general “electronic means of communication” – a phrase that allows for future innovation.

Transactions for workers compensation are dependent upon signatures and approvals from a variety of sources including the claimant, attorneys, physicians and BWC authorities. Consequently, digital signatures were fundamental to the roll-out of the Dolphin network. The verification system depends upon sets of information. Users receive a log-on identity consisting of three initials. This identity is tied to other data such as the user’s policy number, an account number, social security number or perhaps a tax ID number – in the case of an employer. All the information must agree for access to be granted.

³⁶ Darby Patterson interviewed Jim Samual, Chief of Corporate Affairs, Ohio Bureau of Workers’ Compensation. (614-466-2922) jim.Samuel@ohiobwc.com / Dolphin: www.ohiobwc.com

Samuel said the agency developed the user methodology based on familiar elements of the paper-based process. They did not want to introduce new steps in the electronic process, steps that might confuse users or make the system cumbersome. Issues such as fraud and security were considered, but officials decided not to “go overboard” in creating layers of protection. Accepting that some people will be successful in defeating any system – paper or electronic – BWC authorities tried to strike a balance between security and easy access to online services.

Samuel said the electronic process actually has some inherent security extras. There is a trail of communication and documentation that can be tracked in digital transactions, while tracing mailed or faxed paperwork is much more difficult.

The BWC built its own technology using standard IT companies, such as Microsoft and Cisco, to support the system. Since the agency already owned much of the data needed, Samuel said that building the application was a natural step. The department characterizes itself as entrepreneurial and, although it is a public agency, identifies strongly with private-sector business practices. The biggest challenge was to get all the stakeholders to agree on what was needed. There were weekly meetings during development, bringing together the legal community, business owners, medical professionals and the public.

There is overall satisfaction with the use of digital signatures to transform the way BWC serves the public. Nonetheless, the agency is already updating the Web service, asking a new focus group to make suggestions on how to make a good thing, even better. The potential for future growth is impressive. There are about 280,000 businesses in Ohio and 60,000 medical providers that could, according to Samuel, interact with Dolphin. Each could potentially be issued a digital signature.

c. Interview #3: Tamee Roberts, State of Utah, Department of Community and Economic Development³⁷

In 1991, the state of Utah created funding targeted towards improving technology and the use of technology within the state. Ten years after the initial funding pool was created, the Department of Community and Economic Development (DECD) proposed to use the funds to improve its relationships with businesses within and outside the state. DCED believed that many companies across the nation were not willing to go through all of the paperwork required to do business within the state of Utah and to enter into contracts to use existing economic development incentive programs.

In 1999, DCED researched an electronic transaction processing system that would replace the paper-based contracting process. The department’s research identified a

³⁷ Jeff Lemmo and Kol Harvey interviewed Utah state employee, Tamee Roberts, who is with the state of Utah, Department of Community and Economic Development. (801) 538-8704 Troberts@utah.gov.

company called NxLight. NxLight provides marketing solutions for governments and other entities.

NxLight's research had revealed that paper-based processing of financial and business incentive program applications typically extends the contractual process. According to NxLight, a typical process takes "between 10 and 25 days to complete and leaves the parties awash in paper, faxes and FedEx charges... and unnecessary costs created by requiring excessive manual intervention and the collection of 'wet signatures' throughout the process."³⁸

The DCED chose to use NxLight's Incentive Loan Solution to move the contracting process from paper-based to a totally electronic process that uses electronic signatures. The first step was to develop a contract and its related policies and procedures. This proved to be a difficult step for DCED since this was a new process that they were developing and implementing. The DCED put together many drafts of the contract and posted them to the NxLight website, which hosts the state's "Incentive Loan Solution." Companies were invited to test the e-transaction solution in advance. This worked to DCED's advantage because of the important, informative feedback received from the companies that tested the system. Many companies recommended changes, additions and deletions for each draft of the contract posted on the website. The feedback, while useful, meant that DCED posted many drafts of the contract while trying to perfect the transaction. DCED reported that developing the policies, procedures and contract more thoroughly before posting them for review could have avoided many of the revisions.

At the same time that the contract was being posted to the NxLight website, the DCED had companies create user IDs and passwords and test the system by filling out and submitting the beta version of the contract. This testing provided DCED with additional suggestions on how to improve their web site. DCED continued to modify and improve its site throughout the testing phase.

In March of 2002, the state of Utah and its DCED launched the NxLight Incentive Loan Solution. Since the launch, over 20 companies including over 80 users have submitted their electronic contracts for economic development incentive programs sponsored by the state of Utah. DCED reports that the new, paperless contracting process has been a significant improvement over the previous procedures. It has not only cut down the amount of paper the DCED uses, but it has also freed up time and state resources. After eight months using the system, DCED reports that it has seen a return on investment. The project has received recognition from the governor of Utah and built support for similar paperless technologies that could be initiated and launched throughout the state during by the end of 2002.

³⁸ "NxLight Government Solutions," Internet, accessed online at <http://www.nxlight.com/government.jsp>; October 8, 2002.

V. Conclusion

The consistent forward movement of electronic government is an ever-evolving situation, one that often leads to as many problems as novel ideas. We hope you read this paper not just as a research document, but one that may provide new insight and ideas into the electronic and digital signature arena. Sometimes, looking back at a “lesson learned” may lead you into the “new solution”.

Appendix A

The following section provides a detailed explanation and description of state and federal electronic signature legislation and recent court decisions evaluating the enforceability of electronic contracts:

I. Legal Trends

a. Court challenges and questions of how certain terms in the E-SIGN law applies to government

i. Although E-SIGN and UETA Have Not Been Tested in Court, Judges Routinely Enforce Electronic Contracts Based on Basic Contract Principles

As of this writing, no reported decision has been found that interprets the provisions of E-SIGN or the various enactments of UETA in the context of electronic contracting.³⁹ However, numerous cases involving electronic contracts have confirmed the validity of electronic contracts and signatures.

Without turning to an analysis of electronic signature statutes, several courts have analyzed whether “clickwrap” agreements⁴⁰ are valid and binding contracts. So long as the terms are shown to the contracting party, and that party is required to perform some act that indicates an intent to be bound by those terms, courts will likely enforce the contract. For example, in *Moore v. Microsoft Corp.*, 741 N.Y.S.2d 91 (April. 5, 2002), New York Supreme Court analyzed whether a Microsoft End User License Agreement (“EULA”) was a valid, binding contract. *Id.* at 92. The court noted the following:

The terms of the EULA were prominently displayed on the program user’s computer screen before the software could be installed. Moreover, the program’s user was required to indicate assent to the EULA by clicking on the “I agree” icon before proceeding with the download of the software.

Ibid. Based on these facts, the court held that the plaintiff had accepted the terms of the contract by using the software after having an opportunity to read the EULA and, therefore, plaintiff’s claims were barred by the disclaimers, waivers of liability, and limitations of remedies in the license agreement. *Ibid.*

³⁹ In *People v. McFarlan*, 744 N.Y.S.2d 287 (April 4, 2002), the Supreme Court of New York discussed in dicta the difficulties of determining whether E-SIGN pre-empts New York’s Electronic Signatures and Records Act with regard to electronically stored police photographs. The *McFarlan* court ultimately held that it did not need to reach the issue as the electronic records at issue would be valid under either law. *Id.*, 744 N.Y.S.2d at 294-95.

⁴⁰ Common examples of click wrap agreements include online software license agreement or website terms of service agreement.

Several other courts have reached the same result as the *Moore* court. See, e.g., *I. Lan Systems, v. Netscout Service Level Corp.*, 2002 U.S. District LEXIS 209 (D. Mass. January 2, 2002) (held limitation of liability clause in “clickwrap” software license agreement enforceable); *Caspi v. Microsoft Network, LLC*, 323 N.J. Super. 118 (1999) (upholding a forum selection clause in an MSN subscriber agreement where the prospective subscriber was required to click on an “I agree” button next to a scrollable box containing the terms and conditions before proceeding to use the related services); and *Groff v. American Online, Inc.*, 1998 R.I. Super. LEXIS 46 (May 27, 1998) (enforcing forum selection clause in a clickwrap agreement where customer was unable to proceed to use the service without affirmatively selecting “I agree”). In *Forrest v. Verizon Communications, Inc.*, 2002 D.C. App. LEXIS 509, *7-*8 (August 29, 2002) the court upheld the forum selection clause in an on-line Verizon DSL service contract, stating that “[a] contract is no less a contract simply because it is entered into via a computer.”

In contrast, courts have denied the enforceability of electronically displayed license terms where the licensee is not required to assent to the license terms before downloading the subject application. In *Specht v. Netscape Communications, Inc.*, 2002 U.S. App. LEXIS 20714 (2nd Circ. October 1, 2002), the Court of Appeals reviewed the District Court for the Southern District of New York’s denial of a motion to enforce an arbitration provision in Netscape’s software license agreements for its Netscape Communicator and a SmartDownload programs. The plaintiffs in that case alleged that the programs created “cookies” tracking their internet activities that were then transmitted to Netscape allegedly in violation the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. *Specht*, 2002 U.S. LEXIS at *5-*7. The plaintiffs acknowledged that when they downloaded the Netscape Communicator program, they could only proceed after clicking on an acceptance button located on the bottom of a scrollable license agreement. *Id.* at *8-*9. In contrast, the plaintiffs were able to obtain SmartDownload without first assenting to the associated terms and conditions. *Id.* at *11-*14. The Court of Appeal held that the arbitration provision in the SmartDownload license agreement was therefore unenforceable because plaintiffs had not manifested assent to be bound by the terms of that license agreement before obtaining the application. *Id.* at *29-*32.

At least two other courts have reached the same result under similar circumstances. See *Williams v. America Online, Inc.*, 2001 Mass. Super. LEXIS 11 (Feb. 8, 2001) (forum selection clause in AOL’s “terms of service” agreement was not binding because the related software reconfigured the user’s computer before the prospective user was given an opportunity to accept or reject the agreement); *Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 U.S. Dist. LEXIS 4553 (C. D. Cal. March 27, 2000) (Ticketmaster’s online agreement requiring personal use only was not binding on a commercial competitor because affirmative assent was not required before accessing the website services).

As the above cases illustrate, courts will likely enforce electronic contracts so long as a party is required to demonstrate an intent to be bound by the terms of the contract before accessing the goods or services. This evidence can include a simple act like clicking on an “I Agree” button on the screen that provides the terms of the contract.

However, other courts have enforced electronic contracts even though a party did not formally manifest assent by clicking on an “I agree” button. In such cases, the courts have looked to the circumstances of the transaction to determine if the party’s actions provided sufficient evidence to conclude that the parties intended to enter into the contract. *Lim v. The.TV Corp.*, 99 Cal. App. 4th 684 (June 4, 2002), involved an auction for an Internet domain name. The.TV Corporation (“dotTV”) entered into an agreement with the island of Tuvalu to register for a fee Internet domain names using the top-level “tv” domain name, exclusively owned by Tuvalu. *Id.*, 99 Cal. App. 4th at 687. DotTV used a public auction method to sell common names with broad commercial appeal, including the “Golf.tv,” the domain name at issue in the case. Plaintiff Je Ho Lim (“Lim”) was the top bidder for “Golf.tv” with a bid of \$1,010. *Id.* at 687-88. Lim received an email notification, titled “E-MAIL INVOICE FOR DOMAIN REGISTRATION,” that stated “Congratulations! You have won the auction for the following domain name: Domain Name: - - golf.” *Id.* at 688. The email notification also stated that the subscription length was for two years from activation and that dotTV would charge Lim’s credit card for the initial registration fee. *Id.* at 688. Later, DotTV notified Lim that he should “disregard” the email notification, calling it an “email error,” and subsequently offered the name “Golf.tv” for sale with an opening bid of \$1,000,000. *Id.* Lim sought to enforce the contract, relying on the email notification. The trial court dismissed Lim’s complaint for failure to state a cause of action, based on the fact that the email notification stated “- - golf” rather than “golf.” *Id.* at 689.

The court of appeal overturned that decision, holding that Lim had adequately plead the existence of a contract. *Id.* at *8. The court rejected dotTV’s argument that it had effectively rejected all bids and was therefore free to re-bid the domain name:

[E]ven if we were to take [dotTV’s] point and conclude that the website announcement was not an offer but an invitation to make offers, and that plaintiff’s bid was an offer, it was accepted by the e-mail

Id. at 693.

Thus, even in the absence of electronic signature laws, a contract formed electronically may be held to be enforceable under the basic rules governing contract formation. So long as sufficient evidence exists for a court to be able to conclude that a party intended to enter into a contract and be bound by its terms, a court will likely enforce the contract without a need to consider electronic signature statutes. See *Lehman Bros. Inc. v. Canadian Imperial Bank and Comm.*, 2000 U.S. Dist. LEXIS 13979, *38-*39 (S.D. N.Y. 2000) (finding that, in combination, email messages, faxes, and tape recorded telephone call were sufficient to satisfy the statute of frauds in relation to a

\$1.55 billion transaction in U.S. Treasury Notes); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (holding that Register.com's terms of use were binding even though a user was not required to click on an "I agree" button, because the terms of use were posted on the website, those terms stated that submitting data constituted assent to be bound, and Verio had, with knowledge of those terms, submitted data); *Phoenix Renovation Corp. v. Gulf Coast Software, Inc.*, 2000 U.S. Dist. LEXIS 20026 (E.D. V.A. 2000) (upholding an arbitration provision in a software license agreement where an agent of the software vendor had loaded the software, clicking on the "I accept" button, and the buyer had then manifested assent by not thereafter rejecting the software); and *Barman v. Union Oil Company of California*, 1999 U.S. Dist. LEXIS 13973 (D. OR Aug. 13, 1999) (finding emails exchanged between the parties, together with other paper documents, comprised sufficient "writings" to satisfy the statute of frauds and show the parties' intent to be bound).

ii. E-SIGN May Face Judicial Scrutiny In Public Procurements

E-SIGN applies to "any action or set of actions relating to the conduct of business, consumer or commercial affairs between two persons," including government agencies, which are in or affect interstate or foreign commerce. Therefore, E-SIGN appears to apply to a broad array of government activities, i.e. any activities that "relate to business or commercial affairs" that are in or affect interstate commerce.

However, in guidance issued on September 25, 2000, the Office of Management and Budget noted that Congress "specifically rejected" the term "governmental transaction" in the definition of transactions.⁴¹ OMB therefore interpreted "transaction" to exclude activities that are "distinctively governmental."⁴² Accordingly, OMB decided that agencies are not bound by E-SIGN when performing purely governmental functions (e.g., census reporting or administration of government programs).⁴³

Section 104 of E-SIGN explicitly includes certain "Exceptions for Actions by Government as Market Participant."⁴⁴ Therefore, there is no question that Congress intended E-SIGN to apply to government agencies when they act in the marketplace, e.g., through procurement of goods and services. The OMB Guidance confirms that E-SIGN does apply when government agencies choose to engage in transactions of a commercial nature.⁴⁵

Interestingly, the plain language of E-SIGN appears to actually require government agencies, and seemingly no one else, to use electronic signatures in most stages of the contracting cycle. Section 101(b)(2) of the Act provides:

⁴¹ See M-00-15, *Memorandum for the Heads of Departments and Agencies* from Jacob J. Lew, Director, Office of Management and Budget, attaching "OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act (E-SIGN)," September 25, 2000 ("OMB Guidance"), at 3. In contrast, the definition in UETA includes "business, commercial or governmental affairs."

⁴² OMB Guidance at 3.

⁴³ *Ibid.*

⁴⁴ See, 15 U.S.C. §§ 7002(b) and 7004(b)(4).

⁴⁵ *Ibid.*

(b) This title does not -- . . .

(2) require any person to agree to use or accept electronic records or electronic signatures, **other than a governmental agency with respect to a record other than a contract to which it is a party.**⁴⁶

Thus, like UETA, E-SIGN does not force any party to accept an electronic record or signature. But unlike UETA, E-SIGN singles out government agencies, apparently requiring them to use electronic signatures for records other than a actual agency contract. At least two commentators have noted this feature of the statute.⁴⁷

Based on the plain language of Section 101(b)(2), government agencies are arguably required to accept electronic records and signatures in activities that relate to “business, consumer or commercial affairs,” except in relation to an agency’s own contracts. The OMB Guidance even notes that agency commercial transactions (*e.g.*, issuing loan guarantees or mortgage insurance) should be subject to the E-SIGN except with respect to the actual contract with the agency.⁴⁸ The OMB Guidance further states that:

If an activity [by a government agency] involves a ‘transaction’ (generally, the conduct of business, consumer or commercial affairs) that is not a contract, or if it involves a contract to which the agency is not a party, Section 101(a) might require recognition of electronic signatures and records (Section 101(b)(2)) . . .⁴⁹

Government agencies and their contractors engage in many procurement activities that relate to “business or commercial affairs.” Agencies publish solicitations, contractors submit proposals, and many other communications are made in the course of a procurement. These actions relate to business or commercial matters in that they involve the sale of goods or services that are in or affect interstate commerce. Thus, they fall with E-SIGN’s definition of “transaction” and are clearly within the scope of E-SIGN’s applicability. None of these actions constitute “the contract” to which the agency is a party, and therefore E-SIGN would appear to require agencies to use and accept electronic signatures.

Additionally, other records are generated in the course of contract performance that do not constitute the contract with the agency. For example, notices are issued by the contracting parties and reports and other deliverables are submitted. There is nothing in the Act to suggests that such records are not subject to E-SIGN’s mandate requiring the

⁴⁶ 15 U.S.C. § 7001(b)(2) (emphasis added).

⁴⁷ S. Domanowski, *E-SIGN: Paperless Transactions in the New Millenium*, 51 DePaul L. Rev. 619 (2001), n. 207 (“The Act exempts a governmental agency from the voluntary posture of the Act.”); T. Smedinghoff, *Creating Enforceable Electronic Transactions*, n. 24, available at www.bmck.com/eccommerce/article-electronic-transactions.rtf.

⁴⁸ OMB Guidance at 16.

⁴⁹ *Ibid.*

acceptance of electronic records and signatures by a government agency, so long as they “relate to the conduct of business, consumer or commercial affairs” between the agency and its contractor.

However, the OMB Guidance asserts that the exception for an agency’s own contract should be interpreted broadly to include “all records relating to the contract.”⁵⁰ OMB rejected the suggestion that government agencies must accept electronic records and signatures in any document connected with or generated in performance of a government contract.⁵¹

The OMB’s interpretation of the limited mandatory application of E-SIGN, though perhaps well intentioned as an extension of the voluntary nature of E-SIGN, is questionable. First, OMB’s interpretation is not supported by the express language of the statute, which limits the exception to the mandatory use clause to “a contract to which the agency is a party.” Congress could have used broader language, such as “procurement records” or “communications made in performance of a contract” if it intended to enact a more expansive exception. But, Congress appears to have intentionally limited the exception to the contract itself. Moreover, under Section 101(a), E-SIGN’s scope explicitly extends to a “contract, or other record relating to such transaction,” not only the contract itself.⁵² Thus, no apparent reason exists to interpret the word “contract” in Section 101(b)(2) to be coextensive with the broader phrase used in Section 101(a) of the Act (“signature, contract, or other record relating to such a transaction . . .”). Not surprisingly, OMB cites no authority for its broad interpretation of the exception.

Although E-SIGN may require federal and State agencies to use electronic records and signatures for some of their procurement related activities, E-SIGN clearly does not require government agencies to accept any and all electronic records and signatures. E-SIGN Section 104(b)(4) creates an exception to the technology neutral requirement for laws and regulations governing agency procurements.⁵³ Section 104 also allows agencies to specify the format of records and other requirements for conducting electronic transactions when an agency has rule making authority over the transaction.⁵⁴

Whether E-SIGN requires agencies to accept electronic records and signatures involves more than simply an interesting statutory interpretation problem. One can easily imagine a vendor deciding at the last moment to pursue a public contract and submitting an electronic notice (e.g., an email) to the contracting officer in order to not be excluded from competition for failure to submit a written notice of intent to bid. If the agency refused to allow the offeror to participate in the procurement, a protest based on E-SIGN may be justified, and OMB’s broad interpretation of the scope of E-SIGN section 101(b)(2) would be put a judicial test.

⁵⁰ OMB Guidance at 16 n. 9.

⁵¹ *Ibid.*

⁵² Domanowski, 51 DePaul L. Rev at 647 (“It is evident, therefore, that *E-SIGN* extends beyond actual transaction documents to encompass all ancillary records, such as applications, filings, notices and similar documentation”).

⁵³ 15 U.S.C. § 7004(b)(4).

⁵⁴ See OMB Guidance at 16.

Lessons Learned: E-Signatures Statutes Workgroup Members

Anthony Bedwell-Coll - Associate, Government Contracts Practice Group, Rogers Joseph O'Donnell & Phillips, San Francisco, CA

Kirk Buffington – C.P.M., MBA, Manager, Procurement & Materials Management, City of Ft.Lauderdale, FL

Kol Harvey – Management Consultant, Berry Dunn McNeil & Parker, Portland, ME

Neal Hutchko – see below

Jerry Johnson – Senior Policy Analyst, NASIRE

Michele T. Kryszak – Editorial Board, The Internet Law Journal

Jeff Lemmo – Consultant, Berry Dunn McNeil & Parker, Portland, M

Darby Patterson – Editor-in-Chief, Government Technology Magazine

Allen Samelson – Partner, Government Contracts Practice Group, Rogers Joseph O'Donnell & Phillips, San Francisco, CA

Closing note:

What we gained from this experience is that not only did we learn a lot from each other, but made new friends as well. I firmly believe that these types of exercises, utilizing all lines of government and private sector involvement, can help resolve some of the problems and issues that we face as electronic government evolves. No longer is e-government a source for simply providing information, but is now an interactive, secure environment for the consumer/citizen.

Many thanks to the group members who have put in numerous hours and worked through many conference calls to put this paper together. Allen Samelson, Anthony Bedwell-Coll, Darby Patterson, Jeff Lemmo, Jerry Johnson, Kirk Buffington, Kol Harvey, and Michele Kryszak should all be commended for the countless days of research, interviews and writing that went into this document. I am proud to have been a part of this team and found it to be a rewarding endeavor.

Neal Hutchko

Staff Coordinator – National Electronic Commerce Coordinating Council
Policy Analyst – National Association of State Auditors, Comptrollers and
Treasurers