



**Survey of  
Electronic and Digital Signature Legislative Initiatives  
in the United States**

**Prepared for ILPF  
by  
Albert Gidari, Esq.  
John P. Morgan, Esq.  
Perkins Coie**

**September 12, 1997**



# Survey of State Electronic & Digital Signature Legislative Initiatives

## PROJECT OVERVIEW

The Internet Law & Policy Forum ("ILPF") commissioned Perkins Coie to survey current legislative efforts by individual states in the United States and drafting committees concerning digital and electronic signatures to assist the ILPF Digital Signature Working Group in considering model state legislation. This report provides a state-by-state comparison of electronic authentication initiatives and a summary and analysis of trends. The terms of reference of the Working Group and project schedule are available on ILPF's web site <[www.ilpf.org](http://www.ilpf.org)>. The text of all of the state initiatives and related resources have been collected on ILPF's web site as well. ILPF seeks public comment on this report, particularly in regard to the categorization of state initiatives, information on any new initiatives, or corrections to the report. Any comments should be forwarded for consideration to the ILPF via its web site or to the authors of this report, John P. Morgan and Albert Gidari.

## I. BACKGROUND

Legislators are faced with unique and fundamental policy choices regarding the role of government in the development of electronic commerce. Recognizing that government must play a role in enabling electronic commerce by removing traditional barriers, nearly every state has sought to eliminate barriers caused by traditional writing and signature requirements by drafting legislation designed to permit the authentication of documents and signatures through electronic means. In the electronic environment, however, the authentication of documents and signatures is considerably more difficult than in the traditional written environment. An original message may be virtually indistinguishable from a copy, and the potential for fraud is heightened by the ease of alteration.<sup>1</sup>

---

<sup>1</sup> Traditional "writing" requirements serve a host of purposes:

- (1) ensuring that there is tangible evidence of the existence and nature of the intent of the parties to bind themselves;
- (2) to help the parties be aware of the consequences of their entering into a contract;
- (3) to provide a document that is legible to all;
- (4) to provide a permanent record of the transaction that would remain unaltered over time;
- (5) to allow for the reproduction of a document so that each party can have a copy of the same;
- (6) to allow for the authentication of the data by means of a signature;
- (7) to provide a document that is in a form acceptable to public authorities and courts;
- (8) to finalize the intent of the author

New challenges, therefore, arise in determining government's function, if any, in solving problems unique to electronic authentication such as issues of data integrity, non-repudiation, evidentiary standards, choice of technology, liability standards, contractual freedom, consumer protection, and cross-border recognition of electronically signed documents.

In the international arena, numerous governments and organizations have called for private sector leadership in developing electronic commerce principles rather than premature government regulation. However, these policy initiatives also recognize that government may serve an essential facilitating role by eliminating barriers and providing a broad legal framework to protect the interests of the public.<sup>2</sup>

In the United States, 40 states either have considered or enacted electronic authentication laws. Thirteen states have initiated task forces to study the various impacts of electronic commerce and traditional writing and signature requirements. *See* Appendices A & B. Although the numbers suggest that there has been a flurry of substantive activity, in fact, most legislation has been narrow in scope. While 21 states have proposed 31 laws that encompass public and private sector communications ("general" laws), only ten states have enacted 13 such laws. Instead, most legislative activity has involved laws that have a "limited" transactional scope; that is, laws that apply only in a government or narrow private sector context such as the use of electronic signatures by health care providers or for motor vehicle registration. Indeed, twenty-eight states have introduced 48 limited statutes. Of these, 23 states have enacted 36 limited laws. *See* Appendices B & C.

## II. AUTHENTICATION MODELS

A variety of authentication models have been considered or enacted by the states. The vast majority of all legislative initiatives enacted by state legislatures were electronic signature laws while only a handful have enacted digital signature laws.

---

of the writing and provide a record of that intent; (9) to allow for the easy storage of data in tangible form; (10) to facilitate control and subsequent audit for accounting, tax or regulatory purposes; and (11) to bring legal rights and obligations into existence in those cases where a "writing" was required for validity purposes. *See* Illinois Electronic Commerce Security Act, Interim Draft, Cmt. § 202 (June 4, 1997); Guide to Enactment of the UNCITRAL Model law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication ¶ 58 (Apr. 24, 1996).

<sup>2</sup> *See* President William J. Clinton & Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce* (July 1, 1997) <[www.whitehouse.gov](http://www.whitehouse.gov)>; A European Initiative in Electronic Commerce, COM(97)157, at 12-19 (Apr. 4, 1997) <[www.ispo.cec.be/Ecommerce](http://www.ispo.cec.be/Ecommerce)>; Bonn Declaration, European Ministerial Conference: Global Information Networks (July 8, 1997) <[www2.echo.lu/bonn/final.html](http://www2.echo.lu/bonn/final.html)>. A.B.A., *Eliminating Electronic Barriers to Electronic Commerce* (resolution adopted Aug. 1997).

While the distinction between an electronic and digital signature is an important one, the terms frequently are used interchangeably. For purposes of consistent analysis here, "electronic signature" means any identifiers such as letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party to a transaction with an intent to authenticate a writing. A writing, therefore, is deemed to be electronically signed if an electronic signature is logically associated with such writing.<sup>3</sup>

In contrast to an electronic signature, a "digital signature" is an electronic identifier that utilizes an information security measure, most commonly cryptography, to ensure the integrity, authenticity, and nonrepudiation of the information to which it corresponds.<sup>4</sup> Cryptography refers to a field of applied mathematics in which digital information may be transformed into unintelligible code and subsequently translated back into its original form. In public key cryptography or asymmetric cryptography, an algorithmic function is used to create two mathematically related or complementary "keys." One key is used to code the information while the other is used to decode it. Cryptography can be used to ensure the confidentiality of data (i.e., encryption) and to verify the authenticity and integrity of transmitted data. The advantage of public key cryptography is that it allows the confidential transmission of information in open networks where parties do not know one another in advance or share secret key information.

In an open network context, public key encryption depends on the public and private use of these complementary algorithmic keys. The "public" key is associated with a particular party and is made readily available in a directory. A trusted third party or certification authority can authenticate the relationship between a public key and its owner thereby ensuring public confidence in the use of the readily available key. This public key is then used to encrypt a message or data to be sent to the person associated with the key. The recipient of the encrypted message then uses his or her "private" key to decrypt the information. The "private key" is so named because it must remain secret in order for the process to be secure, for while the public key of a particular party is known to the public, only the private key can be used to decrypt. With strong encryption, it is virtually impossible to derive the private key from its public counterpart.

---

<sup>3</sup> See S.B. 942, § 4(4) (Fla. 1996).

<sup>4</sup> A common definition for digital signatures may be found in the Utah Digital Signature Act, Utah Code § 45-3-103(10):

"Digital signature" means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether:

- (a) the transformation was created using the private key that corresponds to the signer's public key; and
- (b) the message has been altered since the transformation was made.

In the context of "digital signatures," the process essentially is reversed. First, a signer uses a "hash" function to create a compressed form of the message to be sent. This "message digest" is unique to the message and can be used subsequently to verify the authenticity of the document once received. Before sending the document electronically, the signer applies the private key to the message digest thereby encrypting it and creating a secure digital signature. The document may then be sent (perhaps encrypted with the receiver's public key) along with the digital signature. Upon receipt, the digital signature can be decrypted with the signer's public code and the message digest can be used to verify the contents of the electronic document. The creation of an open public cryptographic system has commonly been referred to as public key infrastructure ("PKI").<sup>5</sup>

Thirty-three of 49 electronic signature statutes introduced (23 of 28 states) were enacted. Nearly all of these laws were "limited" in scope. With respect to digital signature laws, only ten of 21 initiatives introduced (7 of 14 states) were enacted. Florida, New Hampshire, and Oregon have approved legislation for both. *See* Appendices B & E.

Most of the electronic and digital signature initiatives fall into three categories: prescriptive, criteria-based, and signature enabling. *See* Appendix D. The prescriptive states delineate specific PKI schemes for digital signatures and typically have "general" applicability. Utah's model is predominant among the prescriptive states, accounting for ten of the 18 states using a prescriptive PKI digital signature approach. The criteria-based states recognize the authentication of digital or electronic signatures, provided the signatures satisfy certain criteria of reliability and security. California is the leading model and has been uniformly followed by states utilizing the criteria-based approach. The signature enabling states take the most modest approach by recognizing electronic signatures and documents in a manner that is parallel to traditional signature and writing laws. These laws are technology-neutral in that they adopt no specific technological approach or criteria. Massachusetts has taken the representative lead in this area. These various approaches are discussed in more detail below.

## **A. Prescriptive Approach**

The prescriptive approach is a comprehensive effort that seeks to enable and facilitate electronic commerce with the recognition of digital signatures through a specific regulatory and statutory framework. It establishes a detailed PKI licensing scheme (albeit voluntary), allocates duties between contracting parties, prescribes liability standards, and creates evidentiary presumptions and standards for signature or document authentication.

---

<sup>5</sup> For more information regarding cryptography and PKI, the reader should consult the ILPF digital signature web site <[www.ilpf.org](http://www.ilpf.org)> and the various sources listed there. *See also Secretariat Note, Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues*, UN Commission on International Trade Law, 31st Sess., U.N. Doc. A/CN.9/WG.IV/WP.71 (Dec. 31, 1996).

On the whole, 18 states have adopted or considered PKI-based digital signature laws. Of these, 14 states have addressed digital signatures alone while four states have considered giving effect to both electronic and digital signatures. See Appendix E. California may also be included in this latter category with the recent promulgation of proposed regulations by the Secretary of State that approve of PKI and digital signature use.

The leading model for the prescriptive approach is the Utah Digital Signature Act. Utah Code § 46-3-101 *et seq.* Utah's digital signature law originally was enacted in 1995 and significantly amended in 1996 by Utah Senate Bill 188. This legislation was influenced heavily by the efforts of the American Bar Association Information Security Committee (the "Security Committee"). Over a four-year period, the Security Committee had sought to draft a model law for digital signatures. However, given the diverse views on several key areas such as a subscriber's duty of care, the Security Committee produced the *Digital Signature Guidelines* (the "*Guidelines*") in the summer of 1995 in lieu of a model law.<sup>6</sup> The Utah Digital Signature Act and the *Guidelines* have been very influential in shaping other states' legislative initiatives (together "Utah/*Guidelines*" model).

The Utah/*Guidelines* model attempts to delineate a comprehensive scheme for the recognition of digital signatures in a PKI environment utilizing state-licensed certification authorities ("CAs"). The model can be divided into four main categories: (1) licensing of CAs; (2) issuance, suspension, and revocation of certificates issued by CAs; (3) duties, warranties, and obligations of licensed CAs, subscribers, third parties, and key repositories; and (4) rules regarding the recognition and validity of digital signatures. Some key attributes of these areas include:

- Regulatory authority is vested with the Secretary of State or other agency and may serve as a CA;
- "Voluntary" licensing scheme for CA--unlicensed CAs lose evidentiary presumptions of authenticity and civil liability limitations;
- CAs liability limited by certificate statements; statutorily liable only for direct, compensatory reliance damages;
- A digital signature is self-authenticating if (1) it is verified as valid by a public key listed with a licensed CA; (2) it was affixed with the intention of signing a message; and (3) the recipient has no knowledge of either a breach of duty by the subscriber or does not rightfully hold the private key affixed to the message;

---

<sup>6</sup> Information Security Committee, Electronic Commerce Division, Science & Technology Section, A.B.A., *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, (Aug. 1, 1996).

- Writing requirements are met if (1) the message bears a digital signature and (2) that signature is verified by a valid licensed public key;
- Auditing and bonding requirements for CAs;
- Cross-border recognition for states whose licensing or authorization requirements are *substantially similar* if the Secretary of State recognizes the CAs by rule; and
- Subscribers have a duty of reasonable care in control of private keys and must indemnify CAs.

Although the Utah/*Guidelines* model has received considerable attention, it has not, in fact, been widely followed. Seven states have considered but not adopted the Utah/*Guidelines* model: Hawaii, Maryland, Michigan, New York, Rhode Island, Vermont, and Virginia. Although incorporating most of the model, draft legislation in Virginia and Hawaii notably deleted the cross-border recognition provision. Numerous other states have adopted or considered Utah's definition of a digital signature without adopting the model itself.<sup>7</sup> Minnesota and Washington are the only states to enact the Utah/*Guidelines* model with some variation. See Appendices C & D. For example, Washington has enacted legislation that allows the parties, with some exception, to alter the terms of the statute by contract.<sup>8</sup>

## **B. Alternatives to the Prescriptive-PKI Model**

The Utah/*Guidelines* model likely has not had more impact due to its inherently regulatory and prescriptive nature.<sup>9</sup> By selecting PKI as the baseline for electronic

---

<sup>7</sup> Florida, Illinois, Indiana, Mississippi, New Hampshire, and Oregon all have utilized Utah's definition in their draft legislation. Utah Code § 46-3-103(10) provides:

"Digital signature" means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether:

- (a) the transformation was created using the private key that corresponds to the signer's public key; and
- (b) the message has been altered since the transformation was made.

<sup>8</sup> See Wa. S.B. 5308, § 34 (Wash. 1997). This provision is also included in the *Guidelines* in Section 2.2. These provisions generally allow contracting parties to alter any part of their relationship with the exception of certain rights and duties such as indemnification and warranties. While Utah's statute permits some provisions to be altered by the parties, Utah limits the waiver to certain enumerated provisions.

<sup>9</sup> For a discussion of the drafting process and critical commentary on the *Guidelines* and the Utah Digital Signature Act, see C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 San Diego. L. Rev. 1143 (1996).

authentication, the model may be viewed as technology-forcing. Although it is ostensibly "voluntary," the favorable liability limits and evidentiary presumption associated with state licensing likely will impair alternatives. No presumptions or liability limits are afforded to other technological solutions that may have comparable or superior security or trustworthiness. For this reason, many states have sought legislative alternatives that more broadly address electronic authentication and have more flexibility. Generally, these alternatives utilize a technology-neutral approach and eschew any specific liability regime in order to avoid market-distorting effects in the emerging technology fields of electronic commerce.

Thirty-one states have or are considering 58 statutes that address electronic signature or electronic authentication standards. *See* Appendix E. Fifty-five of these initiatives representing 29 states may be divided between the criteria-based and enabling categories.<sup>10</sup> *See* Appendix D.

### **1. Criteria-Based Approach**

The predominant model for criteria-based laws is the "California" authentication standard. Akin to an evidentiary standard, the California model incorporates some requirements into the definition of an electronic signature in order to satisfy security and trustworthiness concerns. An electronic signature is legally effective if it is:

- a) Unique to the person using it;
- b) Capable of verification;
- c) Under the sole control of the person using it;
- d) Linked to the data in such a manner that if the data is changed the signature is invalidated; and
- e) In conformity with regulations adopted by the appropriate state agency usually the Secretary of State.

Cal. Gov't Code § 16.5(a) (1995). Prior to the model's enactment, the California legislature explicitly considered and rejected the Utah/*Guidelines* model, in part, due to concerns of market distortion and technological neutrality.

---

<sup>10</sup> States with combined laws are included. *See* Appendix E. However, three initiatives from Maine, Nevada, and Ohio are not included because they are prescriptive electronic signature laws. Although considered broadly as electronic signature laws, Maine (S.B. 473) and Nevada (A.B. 386) limit the form of the signature to actual images. Similarly, Ohio (H.B. 243) mandates biometrics or some two-tiered security procedure but does not expressly adopt PKI. All of these bills have been enacted and have a "limited" scope.



The California criteria-based approach has proven quite flexible for various state legislators. The broad criteria may apply both to electronic and digital signatures since it is designed to lay the requirements for trustworthiness and security. For example, the California Secretary of State has recently published its Proposed Digital Signature Regulations, in which it adopts two acceptable technologies: PKI digital signatures and signature dynamics.<sup>11</sup> Indiana has adopted the California criteria as a prerequisite for the recognition of digital signatures. Illinois is considering the criteria as a basis for evaluating whether an electronic signature may be deemed "secure." The first four elements of the California standard also have been used in legislation from New Hampshire, Rhode Island, and Virginia as optional criteria that the trier of fact *may* consider when evaluating the authenticity of an electronic signature.

On the whole, 11 states have 19 initiatives that incorporate the criteria-based approach. Ten states have adopted the California standard into law. *See* Appendix D. Nine of the enacted laws, California's among them, are "limited" in scope. *See* Appendix A. Georgia, Kansas, New Hampshire and Virginia have enacted "general" statutes that use the California criteria-based approach. Electronic signature laws enacted in Georgia and Kansas are unique because the criteria is incorporated into the definition of an electronic signature.<sup>12</sup>

## **2. Signature-Enabling Approach**

The remaining legislative initiatives fall within the signature-enabling category. The "general" laws permit *any* electronic mark that is intended to authenticate a writing to satisfy a signature requirement. *See* Appendix D. The net effect of this approach is to give legal recognition to both digital and electronic signatures for statutory and common law writing and signature requirements.

An early example of this approach is Florida's Electronic Signature Act of 1996, Fla. Stat. § 1.01 (1996 Fla. H.B. 942). The key elements of the operative terms are:

---

<sup>11</sup> Although the California legislature selected a technology-neutral approach, the recently promulgated regulations closely resemble Utah's PKI approach albeit without. So although the statute more closely resembles an electronic signature law on its face, the regulations make it more in the nature of a digital signature statute. The proposed rules are available at <[www.ss.ca.gov/digsig/regs.html](http://www.ss.ca.gov/digsig/regs.html)>.

<sup>12</sup> Despite the fact that the Kansas statute declares to be a digital signature law, the operative definition more closely resembles an electronic signature law. The Kansas Digital Signature Act (1997 Kan. H. B. 2059) provides, in part:

(b) As used in this act, "digital signature" means a computer-created electronic identifier that is: (1) intended by the person using it to have the force and effect of a signature; (2) unique to the person using it; (3) capable of verification; (4) under the sole control of the person using it; and (5) linked to data in such a manner that it is invalidated if the data are changed.

(c) A digital signature may be accepted as a substitute for, and, if accepted, shall have the same force and effect as any other form of signature.

- The word "writing" includes handwriting, printing, typewriting and all other methods and means of forming letters and characters upon paper, stone, wood, or other materials. The word "writing" also includes information which is created or stored in any electronic medium and is retrievable in perceivable form.
- "Electronic signature" means any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing. A writing is electronically signed if an electronic signature is logically associated with such writing.
- Unless otherwise provided by law, an electronic signature may be used to sign a writing and shall have the same force and effect as a written signature.

Massachusetts also is representative. Massachusetts has put forward the most modest position regarding electronic authentication due to similar concerns voiced in California regarding the potential for market distortions and the need for technological neutrality. Massachusetts, however, does not adopt any particular authentication criteria like California in removing signature and writing barriers.<sup>13</sup> Massachusetts' draft legislation provides, in part:

#### Section 1. Definitions.

As used in this chapter, the following terms have the following meaning:

"Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. The term "record" includes, without limitation, electronic records and written records.

"Signed" or "signature" includes electronic and digital signature methods.

#### Section 2. Electronic Records and Signatures.

(a) Where the law requires information to be in writing, that requirement is met by a record. In any legal proceeding, a record shall not be inadmissible in evidence on the sole ground that it is an electronic record. Any duplicate record that accurately reproduces the original record shall be admissible in

---

<sup>13</sup> The Information Technology Division of Massachusetts' Office of the General Counsel maintains an excellent web site discussing its policy efforts and other states' laws at <[www.magnet.state.ma.us/itd/legal/](http://www.magnet.state.ma.us/itd/legal/)>.

evidence as the original itself unless in the circumstances it would be unfair to admit the duplicate in lieu of the original.

(b) Where the law requires a signature of a person, that requirement is met by that person's electronic signature. Where any rule of law requires a signature to be notarized or acknowledged for filing, that rule is satisfied by an electronic signature that meets standards established by the secretary of the commonwealth.

(c) This section shall not apply:

(i) when its application would be inconsistent with the manifest intent of the parties;

(ii) when its application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the law making body or repugnant to the context of the same rule of law, provided that the mere requirement that a record be "in writing" or "written" shall not by itself be sufficient to establish such intent.

Massachusetts' approach also differs from Florida's in its use of a "record" to address writing and signature requirements, which derives from the United Nations Commission on International Trade Law's Model Law on Electronic Commerce ("UNCITRAL Model Law") and is consistent with language used by the National Conference of Commissioners on Uniform State Laws ("NCCUSL") in revising the Uniform Commercial Code ("UCC") Articles 2B and 4B.<sup>14</sup>

On the whole, 27 states have or are considering the enabling approach. Twenty-two states enacted legislation of which five had "general" applicability.<sup>15</sup> The bulk of the initiatives considered remain in the "limited" class. *See* Appendix D. In general, all of these states are silent regarding such issues as certification authority standards, cross-border recognition, and liability issues. The marketplace and existing laws are left to resolve unanswered questions. Although electronic signatures are recognized, no evidentiary presumptions attach to the use of either electronic or digital signatures. This is in sharp contrast to those states that have addressed digital signatures alone. Thus, this

---

<sup>14</sup> *UNCITRAL Model Law on Electronic Commerce*, U.N. Commission on International Trade Law, 29th Sess., U.N. Doc. Supp. No. 17, Articles 5-9 (A/51/17), Annex I (1996), *reprinted at* 36 I.L.M. 197 (1997), *available at* <<http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm>>; G.A. Resolution 51/162, U.N. GAOR, 51st Sess., U.N. Doc. A/RES/51/162 (1996) (adopted). UNCITRAL also is examining the possibility of an international model law. *Secretariat Note, Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues*, U.N. Commission on International Trade Law, 31st Sess., U.N. Doc. A/CN.9/WG.IV/WP.71 (Dec. 31, 1996).

<sup>15</sup> These states include Florida, New Hampshire, Oregon, Texas, and Virginia. Texas and Virginia amended their respective commercial codes with signature-enabling legislation.

approach is merely "enabling" in that the policy objective simply is to remove writing and signature barriers without endeavoring to facilitate any form of development.

### C. Hybrid Approach

Of all the legislation introduced over the past two years, only Florida, Illinois, New Hampshire, and Oregon authored electronic authentication statutes that addressed both electronic and digital signatures. All four give general recognition to electronic signatures and authorize digital signatures in varying degrees of specificity.

The comprehensive draft legislation being circulated by the Illinois Attorney General Commission on Electronic Commerce and Crime falls between the Massachusetts and Utah/*Guidelines* model approach and incorporates aspects of California's criteria-based model.<sup>16</sup> The Illinois draft gives broad recognition to electronic signatures, adopting many provisions of the UNCITRAL Model Law.<sup>17</sup> The legislation creates a new category of electronic signature based on the California criteria model called "secure electronic signatures." Signatures that qualify are accorded rebuttable evidentiary presumptions regarding the genuineness and integrity of the signature. Parties to a transaction may select from a security procedure that is defined by the statute or one that is commercially reasonable and agreed to by the parties.<sup>18</sup>

The "secure status" of a secure electronic signature may be challenged (1) by evidence indicating either that a security procedure authorized by the statute is *generally* not trustworthy or a security procedure agreed to by the parties is not commercially reasonable or implemented in an untrustworthy manner, or (2) by evidence suggesting that the relying party's reliance was not reasonable. Factors affecting the "reasonableness" of a recipient's reliance upon a signature also may be considered, including the relying party's knowledge, course of dealing, and trade usage. The security procedure authorized by the statute is the use of digital signatures. Electronic records that

---

<sup>16</sup> The September 3, 1997 draft may be found at <[www.mbc.com/ds\\_stat.html](http://www.mbc.com/ds_stat.html)>.

<sup>17</sup> The draft also utilizes several of the signature and record provisions and definitions from the Oklahoma Bankers Association Technology Committee Digital Writing and Signature Statute (June 17, 1997 draft), *available at* <[www.abanet.org/buslaw/cyber](http://www.abanet.org/buslaw/cyber)> (last visited Sept. 9, 1997).

<sup>18</sup> With respect to "commercial reasonableness" and echoing UCC Draft Article 4A § 202(c), section 304(b) provides:

The commercial reasonableness of a security procedure agreed upon by the parties is to be determined by the court in light of the purposes of the procedure and the commercial circumstances at the time the parties agreed to adopt the procedure, including the nature of the transaction, sophistication of the parties, volume of similar transactions engaged in by either or both of the parties, availability of alternatives offered but rejected by the party, cost of alternative procedures, and procedures in general use or similar types of transactions.

are signed with digital signatures may constitute a secure electronic record if the digital signature is created and verified by a valid certificate that is considered trustworthy.<sup>19</sup>

The Illinois draft is more flexible and less restrictive than the Utah/*Guidelines* model in creating a PKI scheme, allocating presumptions, and authorizing the use of digital signatures. The Secretary of State is authorized to take several steps to ensure the quality of certificates issued including the adoption of certain security standards for CAs, voluntary licensing, and third party accreditation. Compliance with the Secretary of State's quality control measures will give rise to a rebuttable presumption of trustworthiness, but a default rule also permits trustworthiness to be found by the trier of fact. Like the Utah/*Guidelines* model, the ultimate burden of going forward with some evidence (burden of persuasion) is placed upon the party challenging the integrity of the record or the genuineness of the signature. The important distinction between the Illinois draft and the Utah/*Guidelines* model is that the presumptions generically apply to secure electronic signatures rather than digital signatures exclusively.

There are no express CA auditing or bonding provisions and the Secretary of State is not authorized to serve as a CA. CA liability is not statutorily limited but may be limited by the CA's certification statements. Subscribers have a duty of care (reasonableness) in holding their private keys secure. CAs have a similar duty to use trustworthy methods and may be bound by certain warranties. Like the Washington law, the Illinois draft also has a blanket authorization to vary its terms by agreement, the only other legislative initiative to do so.

NCCUSL also is drafting its Uniform Electronic Transactions Act.<sup>20</sup> The current draft adopts many of the initial enabling provisions of the UNCITRAL Model Law that give legal recognition to electronic signatures and documents (records). In addition, the NCCUSL draft has adopted the Illinois concept of a "secure electronic record" and "secure electronic signature" and utilizes the California criteria as a litmus test before according any evidentiary presumptions. Its definition of "security procedure" is broad and encompasses the familiar UCC concept of commercial reasonability.<sup>21</sup> Unlike the

---

<sup>19</sup> The concepts of "trustworthiness" and "reasonableness" underlie the Illinois draft. For example, under Section 400(16) relating to the digital signature provisions, "trustworthy system" means:

computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended function, and (d) adhere to generally accepted security procedures.

<sup>20</sup> NCCUSL, Uniform Electronic Transactions Act (Aug. 15, 1997 draft), *available at* <[www.law.upenn.edu/library/ulc/ulc.htm](http://www.law.upenn.edu/library/ulc/ulc.htm)>.

<sup>21</sup> The NCCUSL draft has slightly modified the definition of "security procedure" from that contained in the Illinois draft by adding qualifying language regarding commercially reasonable procedures. Section 102(24) provides:

Illinois draft however, the NCCUSL draft makes no attempt to facilitate the development of the prescriptive digital signature/PKI model by linking evidentiary presumptions with digital signatures. The determination of "security" with its associated presumptions stands independently. Overall, the NCCUSL draft endeavors to be more technology-neutral.

### III. CONCLUSIONS

There is no uniformity in state approaches to electronic authentication. States have been most active in deciding appropriate authentication standards for limited transactions with government or discrete areas of private law such as medical records. No electronic authentication model has come to dominate the legislative marketplace and experimentation continues.

This report finds that legislative efforts have been focused predominantly on enacting limited electronic signature laws as opposed to general laws. In the "general" class of statutes, seven states have enacted legislation adopting PKI with three using the Utah/*Guidelines* model; four states have enacted legislation utilizing the California-criteria model of which two use the criteria permissively; and five states have enacted signature-enabling legislation. *See* Appendix D. This contrasts sharply with the 36 limited laws enacted of the 48 proposed during the same time period. *See* Appendix E.

As evidenced by the hybrid approaches of NCCUSL and Illinois, the recent trend is toward legislation that: (a) at a minimum, enables electronic commerce by recognizing that the primary objective of electronic authentication is the removal of barriers associated with traditional writing and signature requirements and (b) establishes evidentiary presumptions in favor of the electronic signature user based on security and trustworthiness standards. The pattern suggests that as security measures increase and provide a heightened indicia of trustworthiness, stronger evidentiary presumptions may attach.

The trend analysis also reveals what is absent from the various state initiatives. For example, only the prescriptive model addresses cross-border recognition of electronic or digital signatures. The Utah/*Guidelines* model only recognizes digital signatures originating in states that have "substantially similar" authentication and licensing

---

"Security procedure," with respect to either an electronic record or electronic signature, means a commercially reasonable procedure or methodology, established by agreement, mutually adopted by the parties, or otherwise established to be commercially reasonable procedure, for verifying (i) the identity of the sender, or source, of an electronic record, or (ii) the integrity of, or detecting errors in, the transmission or informational content of an electronic record. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback or other acknowledgment procedures, key escrow, or any other procedures that are reasonable under the circumstances.

standards and that are recognized by the state regulatory authority by rule. Florida is the only state with a prescriptive statute that requires less and authorizes reciprocity. Additionally, no state initiative addresses choice of law or choice of forum issues with the exception of the NCCUSL draft which essentially adopts conflict of laws common law principles. Thus, there is a legislative gap and no certainty as to whether an electronic signature will be given full force and effect outside of the state on which it was affixed and what law will be used to determine its effect if it is recognized.

Finally, states that have considered or adopted the prescriptive model have uniformly looked to state licensing schemes to ensure trustworthiness. By contrast, Illinois is the only state to consider recognizing the role of non-governmental or private sector third-parties in establishing through accreditation the trustworthiness and security of an electronic authentication.

Albert Gidari, Esq.  
(gidaa@perkins coie.com)  
John P. Morgan, Esq.  
(morgo@perkinscoie.com)  
Perkins Coie  
1201 Third Avenue, 40th Floor  
Seattle, WA 98101  
(206) 583-8888  
(206) 583-8500 (fax)



## Survey of State Electronic & Digital Signature Legislative Initiatives

### Appendix A: Electronic Authentication Summary

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross- Border<sup>7</sup></i>
<i>ALABAMA</i>	None									
<i>ALASKA</i>	None									
<i>ARIZONA</i> 1996 H.B. 2444 (ARS § 41-121)	Enacted	Elec	Accepts filings with Secretary of State (S.O.S.)	L	E			S.O.S.		
<i>ARKANSAS</i>	None									

<sup>1</sup> "Elec"--Electronic Signature; "DSig"--Digital Signature; "Both"--digital & electronic signatures

<sup>2</sup> "L"--"Limited" applicability law; "G"--"General" applicability law

<sup>3</sup> "P"--Prescriptive; "C"--Criteria; "E"--enabling or neutral

<sup>4</sup> "M"--same as Manual; "MC"--same as manual with California standard; "RP"--Rebuttable Presumption

<sup>5</sup> "S"--Subscriber liability = reasonable care, CA Indemnification, and warranties; "CA"--CA liability = limits of certificate, actual damages, and warranties;

<sup>6</sup> "G"--Government CA authorized; "P"--Private party authorized; "L"--Voluntary Licensing; "A"--Auditing authorized; "B&I"--Bonding & Insurance type guarantees required; "O"--Open or not specified

<sup>7</sup> "R"--reciprocity; "C"--Comity = "substantially similar" statute or other standard



<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross-Border<sup>7</sup></i>
<b>CALIFORNIA</b>										
1. 1995 A.B. 1577 (Cal. Gov't Code § 16.5)	Enacted	Elec	Same effect as written if (1) unique to the person using it; (2) capable of verification; (3) under sole control of user; (4) linked to data to allow invalidation; and (5) conforms to Regulations ("California Standard")	L	C	MC		S.O.S.		
Regulations	Public Hearing	Both	Introduces acceptable technologies and allows additions; establishes duties; standards for C.A.s	L	C: approved PKI + Signature Dynamics	MC	S	S.O.S.	L, A	
2. 1997 A.B. 44	Passed 9/2/97	Study	Study by S.O.S. for digital electoral system							
3. 1997 S.B. 49	Committee 8/27/97	Elec	Campaign Filings	L	E					
4. 1997 S.B. 7	Amended 8/05/97	Elec	Candidates for Election--amended version deletes electronic filing provisions	L	E					
5. 1997 A.B. 2755	Enacted	Elec	Applies to Death Certificates	L	E			State Registrar		
6. 1997 A.B. 721	Enacted	Elec	Permits electronic corporate securities filings compliant with California standards	L	C	MC				
7. 1997 S.B. 955	Committee 6/09/97	Elec	Authorizes acceptance by Health Care Service Plan providers	L	C	MC		Comm'r of Corp.		
<b>COLORADO</b>										
1997 S.B. 155	Enacted	Elec	Electronic filing of financial statements	L	E	M		Filing Officer		
<b>CONNECTICUT</b>										
1. Conn. Gen. Stat. §§ 19a-25a	Enacted	Elec	Authorizes regulations for electronic signatures for medical records	L	E			Comm'r of Public Health		

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross-Border<sup>7</sup></i>
2. 1997 S.B. 1308	Died 6/04/97	Study	Task Force to report 1/98							
<b>DELAWARE</b> 458 (29 Del. Code 5942)	Enacted	Elec	Authorizes for state budget and fiscal business	L	E					
<b>FLORIDA</b> 1. Fla. Stat. § 1.01 (1996 S.B. 942)	Enacted	Both & Study	Authorizes use of electronic signatures in lieu of written unless barred by law; permits use of digital signatures via PKI with Secretary of State; Task Force	G	<b>DSig:</b> P <b>Elec:</b> E	RP--if in perceiv- able form		S.O.S.	O	
Committee Report	Submitted	DSig	Recommends S.O.S. to provide voluntary licensure, license and audit fees, insurance/bonding	G	E & P	Same as HB 942	CA (implied)	S.O.S.	G/P, L, A, B&I	C
2. 1997 H.B. 957	Passed House & Carryover 6/11/97	Both	Cyber-notary bill-- authorizes S.O.S. to create notary publics for electronic notarizations	G	E & P		CA (Practice Statement Only)	S.O.S.	G/P, L, A, B&I	R
3. 1997 H.B. 1413	Passed not signed 5/14/97	Both	Similar to H.B. 957	G	E & P					
4. 1997 S.B. 998	Died 6/10/97	Both	Same as H.B. 957	G	E & P					
<b>GEORGIA</b> 1. 1997 S.B. 103	Enacted	Elec & Study	Provides that writing req'ts met where parties agree to accept electronic signatures; encourages electronic commerce; created study	G	C	MC		S.O.S.		

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross-Border<sup>7</sup></i>
2. 1997 H.B. 487	Enacted	Elec	Motor vehicle and traffic use; permits use of "digital signatures" using California standard variation	L	C	MC		Commn'r		
3. 1997 H.B. 479	Enacted	Elec	Tax returns; authorizes regulations for use of electronic notarization	L	E			Commn'r		
<b>HAWAII</b>										
1. HRS 601	Enacted	Study	Study use of digital/electronic signatures in Judiciary Computer Systems							
2. 1997 S.B. 961	Amended 2/28/97	DSig	Based on Utah/ <i>Guidelines</i> Model	G	P	RP	S, CA	Dep't of Commerce	G/P (limited), L, A, B&I	No (C deleted)
<b>IDAHO</b>										
	None									
<b>ILLINOIS</b>										
1. Commission Draft	Not Introduced	Both + Study	Defines "secure" signatures and permits general use; Utilizes UNCITRAL; California Criteria and Utah/ <i>Guidelines</i> Mix	G	E & P	<b>DSig:</b> RP <b>Elec:</b> M	S, CA	S.O.S.(permissive)	O, L, A (optional)	
2. 1997 S.B. 516	Enacted	Elec	Permits use for communications between state agency and comptroller; adopts California standards	L	C	MC		Comptroller		
3. 1997 H.B. 276	Passed House 4/18/97	Elec	Same as S.B. 516	L	C	MC				

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross- Border<sup>7</sup></i>
<b>INDIANA</b>										
1. 1997 S.B. 5a	Enacted	DSig	Effective for state filings other than judicial, legislative, and educational; adopts California standard	L	P--to be adopted	MC		State Board of Accounts		
2. 1997 H.B. 1945	Enacted	DSig	Similar to S.B. 5a	L	P--to be adopted	MC		State Board of Accounts		
<b>IOWA</b>										
1. Iowa Code § 48A.13	Enacted	Elec	Voter registration	L	E			Voter Registration Comm'n		
2. 1997 S.B. 457	Enacted	Elec	Permits electronic signatures for prescriptions; adopts California standard	L	C	MC		N/S		
<b>KANSAS</b>										
1997 H.B. 2059	Enacted	Elec	Permits use of electronic signatures with California recognition standard variation	G	C	MC--If accepted		None	O	
<b>KENTUCKY</b>										
	None									
<b>LOUISIANA</b>										
1. L.R.S. § 40:2144	Enacted	Elec	Medical Records	L	E			Dep't Health & Hospitals		
2. 1997 H.B. 1605	Enacted	Elec	Permits electronic signatures for health care providers on medical records	L	E			Dep't Health & Hospitals		
3. 1997 S.B. 609	Enacted	Elec	Vital records to include electronic documents and signatures	L	E			None		
4. 1997 S.B. 294	Died 8/05/97	Elec	Evidentiary use of electronic bank records and signatures	L	E	M (for certain records)		None		

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross- Border<sup>7</sup></i>
5. 1997 H.B. 1929	Died 8/05/97	Elec	Same as S.B. 609	L	E					
<b>MAINE</b> 1997 S.B. 473	Enacted	Elec	Not true, electronic signature law--permits digital image of signature for motor vehicle code	L	P (signature Image)			S.O.S.		
<b>MARYLAND</b> 1. 1997 H.B. 1015	Died 8/01/97	DSig	Based on Utah/ <i>Guidelines</i> Model	G	P	RP	S, CA	S.O.S.	G/P, L, A, B&I	C
2. 1997 S.B. 822	Died 8/01/97	DSig	Same as H.B. 1015	G	P					
3. 1997 H.B. 1386	Died 8/01/97	Study	Task Force to explore digital signatures, C.A.s, regulation, liability, recognition							
<b>MASSACHUSETTS</b> Draft Bill	Not Introduced	Elec + Study	Recognizes electronic records and signatures with broad criteria	G	E	M		None	O	
<b>MICHIGAN</b> 1997 S.B. 204	Committee 2/19/97	DSig	Based on Utah/ <i>Guidelines</i> Model	G	P	RP	S, CA	Dept. of Consumer & Industry Services	G/P, L, A, B&I	C
<b>MINNESOTA</b> 1. Comprehensive Legislation	Enacted	Elec	Permits limited use of facsimile and digitized signatures in Dep't of Administration (Chpt 16B.05), worker comp. (Chpt. 176.281, 285); tax returns (Chpt. 289A. 07); and motor tax (Chpt. 296.041)	L	E					

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross-Border<sup>7</sup></i>
2. 1997 S.B. 173 (1997 H.B. 56)	Enacted	DSig	Based on Utah/ <i>Guidelines Model</i>	G	P	RP	S, CA	S.O.S.	G/P, L, A, B&I	C
3. 1997 S.B. 1905	Enacted	DSig	Establishes Office of Technology to direct policy; permits use of signatures authorized	L	E	M		Comm'r of Admin.		
4. 1997 H.B. 241	Enacted	Elec	Permits acceptance of electronic signatures for motor carrier documents	L	E	M		Comm'r of Transport.		
5. 1997 S.B. 240	Passed Senate 4/29/97	Elec	Limited use by Dep't of Administration for state business of electronic signatures	L	E	M		Comm'r of Admin.		
6. 1997 H.B. 871	Committee 2/20/97	Elec	Same as S.B. 240	L						
<b>MISSISSIPPI</b>										
1. 1997 H.B. 752	Enacted	DSig	Generic digital signature statute that authorizes S.O.S. to regulate	G	P	RP (implied)		S.O.S.	G/P, L, B&I	
2. 1997 H.B. 1313	Enacted	Elec	Permits filing with S.O.S. electronically	L	E					
3. 1997 S.B. 2904	Died 6/04/97	DSig	Same as H.B. 752	G	P	M		S.O.S.		
<b>MISSOURI</b>										
1997 S.B. 16	Enacted	Elec	Reports by candidates for public offices permitted to be filed electronically if verifiable	L	E					
<b>MONTANA</b>										
1997 H.B. 468	Enacted	Elec	Creates electronic filing system for S.O.S.	L	E			S.O.S.		

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross-Border<sup>7</sup></i>
<b>NEBRASKA</b>										
1. 1997 L.B. 286	Committee 1/16/97	Elec	"Digital signatures" authorized as electronic means of identification utilizing California standard; encourages private use	L	C	MC		S.O.S.		
2. 1997 L.B. 42	Committee 1/10/97	Elec	Similar to L.B. 286; Authorizes the S.O.S. to promulgate regulations	G	C	MC		S.O.S.		
3. 1997 L.R. 262	Introduced 5/22/97	Study	Study of digital signature policy issues							
<b>NEVADA</b>										
1. 1997 A.B. 386	Enacted	Elec	Court clerk may accept image of signature for electronic filing	L	P (signature Image)					
2. 1997 S.B. 42	Enacted	Elec	Permits electronic symbols for facsimile or written signatures for state officers	L	E			Comptroller		
<b>NEW HAMPSHIRE</b>										
1. 1997 S.B. 207	Enacted	Both	Recognizes electronic signatures and authorizes the S.O.S. to create regulations for public and private C.A.s	G	E/C & P	MC (Permissive)		S.O.S.	G/P, L	
2. 1997 H.B. 290	Committee 1/09/97	Both	Permits electronic signatures but provides for digital signatures definition and PKI; Uses Utah definitions	G	E & P	M		S.O.S.--may issue certificates	O, L	
<b>NEW JERSEY</b>										
1997 A.B. 1727	Introduced	Elec	Medical Records authorizations	L	E					

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross-Border<sup>7</sup></i>
<b>NEW MEXICO</b> 1996 H.B. 516 (NMSA §§ 14-15-1 <i>et seq.</i> )	Enacted	DSig	Establishes Office of Electronic Documentation within S.O.S. for C.A. and electronic registrations for transactions with the state Regulations of H.B. 516	L	P	M (Intent to rely)		S.O.S.		
Regulations	Proposed	DSig		L	P		S (keep private only)	S.O.S. & Comm'n of Public Records		
<b>NEW YORK</b> 1997 S.B. 2238 (1997 A.B. 6813)	Committee 2/05/97	DSig	Based on Utah/ <i>Guidelines Model</i>	G	P	RP	S, CA	S.O.S.	G/P, L, A, B&I	C
<b>NORTH CAROLINA</b> 1. 1997 H.B. 290	Committee 2/20/97	Study	Study of electronic commerce issues including signatures and C.A.s Study of electronic commerce policy and feasibility for state agencies Protection of health information to extend to electronic and digital signatures with UCC, ABA and NCCUSL type standards							
2. 1997 H.B. 1047	Committee 4/20/97	Study								
3. 1997 H.B. 925 (1997 A.B. 1005)	Committee 5/20/97	Elec		L	E					
<b>NORTH DAKOTA</b> 1. 1997 S.C.R. 4024	Enacted	Study	Study for state records management and email Authorizes the S.O.S. to adopt rules for signature recognition for tax and motor vehicle registration							
2. 1997 S.B. 2071	Enacted	Elec		L	E			S.O.S.		



<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross-Border<sup>7</sup></i>
<b>OHIO</b> 1997 H.B. 243	Committee 6/10/97	Elec	Authorizes use for Medical Records	L	P	M				
<b>OKLAHOMA</b> 1. Bankers Association Draft	Not Introduced	Elec	Recognizes the use of electronic records and signatures	G	E	M				
2. 1997 H.B. 1690	Enacted	Study	Task Force							
<b>OREGON</b> 1. 1997 S.B. 125	Enacted	Both	Trust companies may use digital & electronic signatures and serve as authentication authorities	L	E & P					
2. 1997 H.B. 3046	Enacted	Both	Permits electronic signatures but provides for digital signatures definition and PKI Amended version authorizes licensing scheme for C.A.s	G	<b>DSig:</b> P <b>Elec:</b> E	M (if listed by Dep't)		Dep't of Consumer & Business Services	O, L	
<b>PENNSYLVANIA</b>	None									
<b>RHODE ISLAND</b> 1. 1997 H.B. 6118	Enacted	Elec	Authorizes electronic signatures and communications for state agencies	L	E/C	MC (Permissive)		S.O.S.		
2. 1997 S.B. 612	Introduced	DSig	Based on Utah/ <i>Guidelines Model</i> ; S.O.S. to implement	G	P	RP	S, CA	Division of Public Utilities	G/P, L, A, B&I	C
<b>SOUTH CAROLINA</b>	None									
<b>SOUTH DAKOTA</b>	None									

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross-Border<sup>7</sup></i>
<b>TENNESSEE</b> 1997 H.B. 1718 (1997 S.B. 1090)	Enacted	Elec	Judicial use authorized for filings	L	E			Courts		
<b>TEXAS</b> 1. 1997 H.B. 984	Enacted	Elec	Authorizes use of electronic signatures to authenticate electronic communications; prescribes California standard for transactions with state	G(UC C) + L	E/C	<b>UCC: M</b> <b>State:MC</b>		Comptroller; state auditor; A.G.		
2. 1997 H.B. 645	Enacted	Elec	Authorizes use of "digital signatures" submitted to comptroller	L	E	M		Comptroller		
3. 1997 S.B. 370	Enacted	Elec	Authorizes use of "digital signatures" for license applications	L	C	MC				
4. 1997 S.B. 748 (1997 S.B. 787)	Died 8/06/97	Elec	Same as H.B. 984 but limited to state agencies	L	C	MC		Comptroller; state auditor; A.G.		
<b>UTAH</b> 1. Utah Code § 45-3-101 <i>et seq.</i>	Enacted	DSig	Creates C.A. licensing scheme; regulations; liability ("Utah/ <i>Guidelines Model</i> ")	G	P	M		Dep't of Commerce	L	
2. 1996 S.B. 188	Enacted	DSig	Major amendment to Digital Signature Act to define terms, req'ts, enforcement, etc. "Digital Signature" defined as using asymmetric cryptosystem to determine whether (a) signature was created using correct private key and (b) message has been altered	G	P	RP	S, CA	Div. Corp. Comm. Code	G/P, L, A, B&I	C

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross-Border<sup>7</sup></i>
Regulations R154-10	Draft	DSig	Set certificate, practice statement, guarantee standards	G	P			Div. Corp. Comm. Code		
4. 1997 H.B. 95	Died 3/05/97	Notary	Sets standards for cyber-notary	G						
<b>VERMONT</b> 1997 H.B. 60	Committee 1/14/97	DSig	Based on Utah/ <i>Guidelines Model</i>	G	P	RP	S, CA	S.O.S.	G/P, L, A, B&I	C
<b>VIRGINIA</b> 1. 1996 H.J.R. 195 2. 1997 S.B. 923	Enacted Enacted	Study Elec	Study Authorization Amends commercial code to recognize signature if "intended"; Council to draft regulations for public transactions	G	E/C	UCC: MC (permissive)		Council on Information Management for public transactions		
3. 1997 H.B. 822	Introduced	DSig	Based on Utah/ <i>Guidelines Model</i>	G	P	RP	S, CA	Corporate Comm'n	G/P (limited), L, A, B&I	No (C removed)
4. 1997 H.B. 2138	Enacted	Study	Study Group							
<b>WASHINGTON</b> 1. 1996 S.B. 6423 2. 1997 S.B. 5308	Enacted Enacted	DSig DSig	Based on Utah/ <i>Guidelines Model</i> Amends S.B. 6423; S.O.S. no longer authorized to be CA; parties may vary by agreement	G G	P P	RP RP (Person need not accept)	S, CA S (unless certificate expired), CA (includes lost profits)	S.O.S. S.O.S.	G/P, L, A, B&I P, L, A, B&I	C
WAC § 434-200	Proposed 9/3/97	DSig	Proposed regulations for CAs and repositories	G	P	RP		S.O.S.	P, L, A, B&I	
<b>WEST VIRGINIA</b>	None									
<b>WISCONSIN</b>	None									

<i>State Initiative</i>	<i>Status</i>	<i>Type<sup>1</sup></i>	<i>Description</i>	<i>Use<sup>2</sup></i>	<i>Class<sup>3</sup></i>	<i>Effects<sup>4</sup></i>	<i>Liability<sup>5</sup></i>	<i>Authority</i>	<i>C.A.s Attributes<sup>6</sup></i>	<i>Cross- Border<sup>7</sup></i>
<b>WYOMING</b> Wyo. Stat. 9-1-306	Enacted	Elec	Authorizes electronic filing with S.O.S.; extends civil and criminal liability	L	E			S.O.S.		



# Survey of State Electronic & Digital Signature Legislative Initiatives

## APPENDIX B: SUMMARY OVERVIEW

<i>State Initiative</i>	<i>Status</i>	<i>Study</i>	<i>Electronic</i>	<i>Digital</i>	<i>General</i>	<i>Limited</i>
<b>ALABAMA</b>	None					
<b>ALASKA</b>	None					
<b>ARIZONA</b>						
1996 H.B. 2444 (ARS § 41-121)	Enacted		,			,
<b>ARKANSAS</b>	None					
<b>CALIFORNIA</b>						
1. 1995 A.B. 1577 (Cal. Gov't Code § 16.5)	Enacted		,			,
1997 Regulations	Public Hearing		,	,		,
2. 1997 A.B. 44	Passed 9/2/97	,				
3. 1997 S.B. 49	Committee 8/27/97		,			,
4. 1997 S.B. 7	Amended 8/05/97		,			,
5. 1997 A.B. 2755	Enacted		,			,
6. 1997 A.B. 721	Enacted		,			,
7. 1997 S.B. 955	Committee 6/09/97		,			,
<b>COLORADO</b>						
1997 S.B. 155	Enacted		,			,
<b>CONNECTICUT</b>						
1. Conn. Gen. Stat. §§ 19a-25a	Enacted		,			,
2. 1997 S.B. 1308	Died 6/04/97	,				
<b>DELAWARE</b>						
458 (29 Del. Code 5942)	Enacted		,			,
<b>FLORIDA</b>						
1. 1996 S.B. 942	Enacted	,	,	,	,	
Committee Report	Submitted	,		,	,	

<i>State Initiative</i>	<i>Status</i>	<i>Study</i>	<i>Electronic</i>	<i>Digital</i>	<i>General</i>	<i>Limited</i>
2. 1997 H.B. 957	Passed House & Carryover 6/11/97		,	Notary	,	
3. 1997 H.B. 1413	Passed not signed 5/14/97		,	Notary	,	
4. 1997 S.B. 998	Died 6/10/97		,	Notary	,	
<b>GEORGIA</b>						
1. 1997 S.B. 103	Enacted	,	,		,	
2. 1997 H.B. 487	Enacted		,			,
3. 1997 H.B. 479	Enacted		,			,
<b>HAWAII</b>						
1. HRS 601	Enacted	,				
2. 1997 S.B. 961	Committee 3/06/97			,	,	
<b>IDAHO</b>						
None						
<b>ILLINOIS</b>						
1. Commission Draft (9/2/97 draft)	Not Introduced	,	,	,	,	
2. 1997 S.B. 516	Enacted		,			,
3. 1997 H.B. 276	Passed House 4/18/97		,			,
<b>INDIANA</b>						
1. 1997 S.B. 5a	Enacted			,		,
2. 1997 H.B. 1945	Enacted			,		,
<b>IOWA</b>						
1. Iowa Code § 48A.13	Enacted		,			,
2. 1997 S.B. 457	Enacted		,			,
<b>KANSAS</b>						
1997 H.B. 2059	Enacted		,		,	
<b>KENTUCKY</b>						
None						
<b>LOUISIANA</b>						
1. L.R.S. § 40:2144	Enacted		,			,
2. 1997 H.B. 1605	Enacted		,			,
3. 1997 S.B. 609	Enacted		,			,
4. 1997 S.B. 294	Died 8/05/97		,			,
5. 1997 H.B. 1929	Died 8/05/97		,			,

<i>State Initiative</i>	<i>Status</i>	<i>Study</i>	<i>Electronic</i>	<i>Digital</i>	<i>General</i>	<i>Limited</i>
<b>MAINE</b>						
1997 S.B. 473	Enacted		,			,
<b>MARYLAND</b>						
1. 1997 H.B. 1015	Died 8/01/97			,	,	
2. 1997 S.B. 822	Died 8/01/97			,	,	
3. 1997 H.B. 1386	Died 8/01/97	,				
<b>MASSACHUSETTS</b>						
Draft Bill (4/17/97 Draft)	Not Introduced	,	,		,	
<b>MICHIGAN</b>						
1997 S.B. 204	Committee 2/19/97			,	,	
<b>MINNESOTA</b>						
1. Comprehensive Legislation	Enacted		,			,
2. 1997 S.B. 173 (1997 H.B. 56)	Enacted			,	,	
3. 1997 S.B. 1905	Enacted			,		,
4. 1997 H.B. 241	Enacted		,			,
5. 1997 S.B. 240	Passed Senate 4/29/97		,			,
6. 1997 H.B. 871	Committee 2/20/97		,			,
<b>MISSISSIPPI</b>						
1. 1997 H.B. 752	Enacted			,	,	
2. 1997 H.B. 1313	Enacted		,			,
3. 1997 S.B. 2904	Died 6/04/97			,	,	
<b>MISSOURI</b>						
1997 S.B. 16	Enacted		,			,
<b>MONTANA</b>						
1997 H.B. 468	Enacted		,			,
<b>NEBRASKA</b>						
1. 1997 L.B. 286	Committee 1/16/97		,			,
2. 1997 L.B. 42	Committee 1/10/97		,		,	
3. 1997 L.R. 262	Introduced 5/22/97	,				

<i>State Initiative</i>	<i>Status</i>	<i>Study</i>	<i>Electronic</i>	<i>Digital</i>	<i>General</i>	<i>Limited</i>
<b>NEVADA</b>						
1997 A.B. 386	Enacted		,			,
1997 S.B. 42	Enacted		,			,
<b>NEW HAMPSHIRE</b>						
1. 1997 S.B. 207	Enacted		,	,	,	
2. 1997 H.B. 290	Committee 1/9/97		,	,	,	
<b>NEW JERSEY</b>						
1997 A.B. 1727	Introduced		,			,
<b>NEW MEXICO</b>						
1996 H.B. 516 (NMSA §§ 14-15-1 <i>et seq.</i> )	Enacted			,		,
Regulations	Proposed			,		,
<b>NEW YORK</b>						
1997 S.B. 2238 (1997 A.B. 6813)	Committee 2/05/97			,	,	
<b>NORTH CAROLINA</b>						
1. 1997 H.B. 290	Committee 2/20/97	,				
2. 1997 H.B. 1047	Committee 4/20/97	,				
3. 1997 H.B. 925 (1997 A.B. 1005)	Committee 5/20/97		,			,
<b>NORTH DAKOTA</b>						
1. 1997 S.C.R. 4024	Enacted	,				
2. 1997 S.B. 2071	Enacted		,			,
<b>OHIO</b>						
1997 H.B. 243	Committee 6/10/97		,			,
<b>OKLAHOMA</b>						
1. Bankers Association Draft (6/17/97 Draft)	Not Introduced		,		,	
2. 1997 H.B. 1690	Enacted	,				
<b>OREGON</b>						
1. 1997 S.B. 125	Enacted		,	,		,
2. 1997 H.B. 3046	Enacted		,	,	,	
<b>PENNSYLVANIA</b>	None					
<b>RHODE ISLAND</b>						
1. 1997 H.B. 6118	Enacted		,			,



<i>State Initiative</i>	<i>Status</i>	<i>Study</i>	<i>Electronic</i>	<i>Digital</i>	<i>General</i>	<i>Limited</i>
2. 1997 S.B. 612	Introduced			,	,	
<b><i>SOUTH CAROLINA</i></b>	None					
<b><i>SOUTH DAKOTA</i></b>	None					
<b><i>TENNESSEE</i></b>						
1997 H.B. 1718 (1997 S.B. 1090)	Enacted		,			,
<b><i>TEXAS</i></b>						
1. 1997 H.B. 984	Enacted		,		,	,
2. 1997 H.B. 645	Enacted		,			,
3. 1997 S.B. 370	Enacted		,			,
4. 1997 S.B. 748 (1997 S.B. 787)	Died 8/06/97		,			,
<b><i>UTAH</i></b>						
1. Utah Code § 45-3-101 <i>et seq.</i>	Enacted			,	,	
2. 1996 S.B. 188	Enacted			,	,	
Regulations R154-10	Draft			,	,	
4. 1997 H.B. 95	Died 3/05/97			Notary	,	
<b><i>VERMONT</i></b>						
1997 H.B. 60	Committee 1/14/97			,	,	
<b><i>VIRGINIA</i></b>						
1. 1996 H.J.R. 195	Enacted	,				
2. 1997 S.B. 923	Enacted		,		,	
3. 1996 H.B. 822	Introduced			,	,	
4. 1997 H.B. 2138	Enacted	,				
<b><i>WASHINGTON</i></b>						
1. 1996 S.B. 6423	Enacted			,	,	
2. 1997 S.B. 5308	Enacted			,	,	
WAC § 434-200	Proposed 9/3/97			,	,	
<b><i>WEST VIRGINIA</i></b>	None					
<b><i>WISCONSIN</i></b>	None					
<b><i>WYOMING</i></b>						
Wyo. Stat. 9-1-306	Enacted		,			,





# Survey of State Electronic & Digital Signature Legislative Initiatives

## APPENDIX C: TRANSACTIONAL SCOPE<sup>1</sup>

<u>General Application (31)</u>		<u>Limited Application (48)</u>		<u>State Studies (13)</u>
Florida*	(4)	Arizona*	(1)	California
Georgia*	(1)	California*	(6)	Connecticut
Hawaii	(1)	Colorado*	(1)	Florida*
Illinois	(1)	Connecticut	(1)	Georgia*
Kansas*	(1)	Delaware*	(1)	Hawaii*
Maryland	(2)	Georgia*	(2)	Illinois*
Massachusetts	(1)	Illinois*	(2)	Maryland
Michigan	(1)	Indiana*	(2)	Massachusetts*
Minnesota*	(1)	Iowa*	(2)	Nebraska
Mississippi*	(2)	Louisiana*	(5)	North Carolina
Nebraska	(1)	Maine*	(1)	North Dakota*
New Hampshire*	(2)	Minnesota*	(5)	Oklahoma*
New York	(1)	Mississippi*	(1)	Virginia*
Oklahoma	(1)	Missouri*	(1)	
Oregon*	(1)	Montana*	(1)	
Rhode Island	(1)	Nebraska	(1)	
Texas*	(1)	Nevada*	(2)	
Utah*	(3)	New Jersey	(1)	
Vermont	(1)	New Mexico*	(1)	
Virginia*	(2)	North Carolina	(1)	
Washington*	(2)	North Dakota*	(1)	
		Ohio	(1)	
		Oregon*	(1)	
		Rhode Island*	(1)	
		Tennessee*	(1)	
		Texas*	(3)	
		Virginia*	(1)	
		Wyoming*	(1)	

---

<sup>1</sup> \* have enacted legislation or have on-going study; (#)--number of initiatives



# Survey of State Electronic & Digital Signature Legislative Initiatives

## APPENDIX D: LEGISLATIVE APPROACHES<sup>1</sup>

### PKI/Digital Signature Approaches

<u>Utah/Guidelines Prescriptive-Based (14)</u>	<u>Broadly PKI Prescriptive-Based (15)</u>
(G) Hawaii (1)	(L) California (Regs.) (1)
(G) Maryland (2)	(G) Florida* (4)
(G) Michigan (1)	(G) Illinois (1)
(G) Minnesota* (1)	(L) Indiana* (2)
(G) New York (1)	(G) Mississippi* (2)
(G) Rhode Island (1)	(G) New Hampshire* (2)
(G) Utah* (3)	(L) New Mexico* (1)
(G) Vermont (1)	(G) Oregon* (1)
(G) Virginia (1)	(L) Oregon* (1)
(G) Washington* (2)	

### Other Approaches to Authentication: Criteria & Enabling

<u>Limited California Criteria Based (13)</u>	<u>General California Criteria Based (6)</u>	<u>Limited Signature Enabling (30)</u>	<u>General Signature Enabling (12)</u>
California* (3)	Georgia* (1)	Arizona* (1)	Florida* (4)
Georgia* (1)	Illinois (1)	California* (3)	Illinois (1)
Illinois* (2)	Kansas* (1)	Connecticut* (1)	Massachusetts (1)
Indiana* (dsig) (2)	Nebraska (1)	Colorado* (1)	New Hampshire* (2)
Iowa* (1)	New Hampshire* (1)	Delaware* (1)	Oklahoma (1)
Nebraska (1)	Virginia* (1)	Georgia* (1)	Oregon* (1)
Rhode Island* (1)		Iowa* (1)	Texas* (1)
Texas* (2)		Louisiana* (5)	Virginia* (1)
		Minnesota* (4)	
		Mississippi* (1)	
		Missouri* (1)	
		Montana* (1)	
		Nevada* (1)	
		New Jersey (1)	
		North Carolina (1)	
		North Dakota* (1)	
		Oregon* (1)	
		Rhode Island* (1)	
		Tennessee* (1)	
		Texas* (1)	
		Wyoming* (1)	

<sup>1</sup> \* enacted legislation; "L"--limited application legislation ; "G"--general application legislation; (#)--number of initiatives



# Survey of State Electronic & Digital Signature Legislative Initiatives

## APPENDIX E: ELECTRONIC VS. DIGITAL SIGNATURES<sup>1</sup>

<u>Electronic Signature Laws (49)</u>	<u>Digital Signature Laws (22)</u>	<u>Combination Laws (9)</u>
(L) Arizona* (1)	(L) California (regs) (1)	(G) Florida* (4)
(L) California* (6)	(G) Hawaii (1)	(G) Illinois (1)
(L) Colorado* (1)	(L) Indiana* (2)	(G) New Hampshire* (2)
(L) Connecticut* (1)	(G) Maryland (2)	(L) Oregon* (1)
(L) Delaware* (1)	(G) Michigan (1)	(G) Oregon* (1)
(G) Georgia* (1)	(G) Minnesota* (1)	
(L) Georgia* (2)	(L) Minnesota* (1)	
(L) Illinois* (2)	(G) Mississippi* (2)	
(L) Iowa* (2)	(L) New Mexico* (1)	
(G) Kansas* (1)	(G) New York (1)	
(L) Louisiana* (5)	(G) Rhode Island (1)	
(L) Maine* (1)	(G) Utah* (3)	
(G) Massachusetts (1)	(G) Vermont (1)	
(L) Minnesota* (4)	(G) Virginia (1)	
(L) Mississippi* (1)	(L) Virginia* (1)	
(L) Missouri* (1)	(G) Washington* (2)	
(L) Montana* (1)		
(G) Nebraska (1)		
(L) Nebraska (1)		
(L) Nevada* (2)		
(L) New Jersey (1)		
(L) North Carolina (1)		
(L) North Dakota* (1)		
(L) Ohio* (1)		
(G) Oklahoma (1)		
(L) Rhode Island* (1)		
(L) Tennessee* (1)		
(G) Texas* (1)		
(L) Texas* (3)		
(G) Virginia* (1)		
(L) Wyoming* (1)		

---

<sup>1</sup> \* enacted legislation; (#) -- indicates number of initiatives; "L"--limited application legislation; "G"--general application legislation