



**UPDATE: 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 LLP**

April 7, 1998



UPDATE: Survey of State Electronic & Digital Signature Legislative Initiatives

INTRODUCTION

This update is a supplement to ongoing efforts of the Internet Law & Policy Forum ("ILPF") regarding the various legislative initiatives in electronic authentication. ILPF commissioned Perkins Coie to survey current legislative efforts by individual states in the United States and various drafting committees concerning digital and electronic signatures to assist the ILPF Digital Signature Working Group ("Working Group") in considering model state legislation. Its initial report, submitted on September 12, 1997, provided a state-by-state comparison of electronic authentication initiatives and a summary and analysis of trends. The report revealed a patchwork of inconsistent state regulation and an absence of standards for the cross-border recognition of electronic signatures. In response, ILPF convened a working-group meeting of experts on electronic authentication issues on October 23-24, 1997. From this meeting and subsequent public commentary, the ILPF produced its Electronic Authentication Principles which represent a broad consensus on several key issues impacting electronic and digital signature laws. Reference should be made to these previous documents for further background and work product of the Working Group's efforts.¹

SUMMARY OBSERVATIONS

A. State Initiatives

With the exception of Arkansas, South Carolina, and South Dakota, all states have considered or enacted some form of electronic authentication law. *See* Appendices B, and C. Overall, 36 states have introduced or are considering 76 electronic signature initiatives. Twenty-six states have enacted one or more of these initiatives into law. In the area of digital signatures or other public key-styled ("PKI") technologies, 20 states have introduced or considered 36 different initiatives or regulations with 10 states adopting some form into law. Seven states are examining laws that address both digital and electronic signatures. *See* Appendix F. Sixteen states have initiated task forces or studies to examine future legislation. *See* Appendix D.

Among these initiatives, most of the activity involves laws with a "limited" transactional scope; i.e. laws that only apply to government or select private sector

¹ The terms of reference of the Working Group, project schedule, report, and resulting principles are available on ILPF's web site <www.ilpf.org>. The text of all the state initiatives and related resources have been collected on ILPF's web site as well.

transactions. Thirty-eight states have introduced 74 limited initiatives. Of these, 29 states have enacted 43 limited laws. In contrast, 30 states have considered 44 initiatives for "general" transactions; i.e. transactions that encompass both public and private sector communications. Thirteen states have enacted 18 general laws. *See Appendix D.*

All three categories of "general" electronic authentication laws (prescriptive, criteria-based, and signature enabling) have seen activity since the initial report. First, 14 states have introduced 22 prescriptive initiatives with only 4 states enacting some form thereof. Minnesota and Washington remain the only states to follow Utah's digital signature statute; however, seven other states have or are considering the Utah model. Missouri represents the latest. Next of the criteria-based general initiatives, eight states introduced nine laws and four of these states have adopted initiatives into law. The criteria established by California Government Code § 16.5 (1995) remains the standard for criteria-based laws, general or limited. Last, signature-enabling initiatives have become increasingly popular. In the general enabling class, 14 states have considered 16 initiatives, enacting 7 into law. Most notably since the last survey, six new initiatives were identified in Colorado, Iowa, Kentucky, Maine, Tennessee, and West Virginia. However, the signature provision in Colorado was later removed. *See Appendix E.*

The first ILPF survey observed that a newly emerging class of statutes, designated as hybrid statutes, addresses both digital and electronic signatures and has components of all the types of laws discussed above. To date in the general hybrid class, six states have considered laws of which three have been enacted (in Florida, New Hampshire, and Oregon). The comprehensive draft legislation being circulated by the Illinois Attorney General Commission on Electronic Commerce and Crime, which has now been introduced as Illinois H.B. 3180, is representative of this approach.² The Illinois approach gives broad recognition to electronic signatures, adopting many provisions of the United Nations Commission on International Trade Law's ("UNCITRAL") Model Law on Electronic Commerce.³ 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.

This approach has recently been followed in several other forums. In Iowa, House Bill 2474 has been introduced adopting the Illinois Commission's final December 1997 draft. In its previous draft, the Uniform Electronic Transactions Act ("ETA") being circulated by National Conference of Commissioners on Uniform State Laws ("NCCUSL") also was quite similar to the Illinois draft. However, the NCCUSL draft recently has been modified by deleting the separate provisions concerning secure

² The Commission's draft, H.B. 3180, and a comprehensive summary of electronic authentication initiatives are available at <<http://www.mbc.com>>.

³ *See* UNCITRAL's home page on electronic commerce at <<http://www.un.or.at/uncitral/>>.

electronic signatures.⁴ The draft still retains some recognition of "security procedures" for purposes of establishing attribution and is consistent with the approach taken by NCCUSL in the revisions of the Uniform Commercial Code Article 2B. The rejection of the concept of secure electronic signature along with its evidentiary presumptions was a significant deviation from prior drafts. Notwithstanding, this may largely be semantic given the introduction of new attribution provisions. This activity highlights the leading debate regarding the proper role of evidentiary presumptions and electronic authentication in general. Whether NCCUSL will afford heightened evidentiary presumptions to "high-security" methods of electronic authentication has yet to be finally decided. Due to pressure from state and federal lawmakers, NCCUSL will continue to evaluate its draft on a fast track and hopes to deliver a final draft in August 1999. NCCUSL will be addressing a new draft in meetings scheduled for mid-April.

On the international front, UNCITRAL also adopted much of the Illinois scheme for consideration in its December 12, 1997 draft of its Uniform Rules on Electronic Signatures ("Uniform Rules").⁵ While it is focusing on the preparation of specific provisions addressing digital signature technique, the Working Group has reiterated its goal to extract rules of more general application from those specific provisions in order to accommodate alternative authentication techniques and to remain more technology- and media-neutral. In January 1998, the Working Group revisited the December draft of the Uniform Rules; this draft has largely retained the concept of secure electronic signatures to ensure this goal.⁶ While NCCUSL has substantially modified the Illinois approach, UNCITRAL appears to have preserved the key concepts of the Illinois draft. Nevertheless, UNCITRAL continues to assess the proper role of evidentiary presumptions and the desirability of technically neutral language.

In view of the new-hybrid styled statutes of Illinois and the early NCCUSL draft, the initial ILPF report concluded that the electronic authentication trend was 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 suggested that as security measures increase and provide a heightened indicia of trustworthiness, stronger evidentiary presumptions may

⁴ NCCUSL, Uniform Electronic Transactions Act (Nov. 25, 1997 draft), *available at* <www.law.upenn.edu/library/ulc/ulc.htm>. A new draft should be made available in April which will contain the revisions discussed in NCCUSL's January meeting.

⁵ Draft Uniform Rules On Electronic Signatures, U.N. Commission on International Trade Law, 31st Sess., U.N. Doc. A/CN.9/WG.IV/WP.73 (Dec. 12, 1997), *available at* <<http://www.un.or.at/uncitral/texts/electcom/>>.

⁶ Report of the Working Group on Electronic Commerce on the Work of Its Thirty-Second Session, U.N. Commission on International Trade Law, 32d Sess, U.N. Doc. A/CN.9/446 (Feb. 11, 1998), *available at* <<http://www.un.or.at/uncitral/sessions/unc/unc-31/acn9-446.htm>>.

attach. This conclusion now appears to be supported by recent developments in Iowa and UNCITRAL.

B. Federal Initiatives

While the states have been very active in submitting diverse electronic authentication laws, Congress has started to examine its role in designating a federal standard or preempting state law, most likely out of concern over the increasing body of inconsistent state laws. The following is a brief summary of the four federal initiatives recently introduced. *See* Appendix A.

On October 21, 1997, Representative Archer (R-TX) introduced H.R. 2676 to reform various aspects of the tax code and the Internal Revenue Service (the "IRS"). As part of the bill's strategic plan to have 80% of all filing performed electronically by 2007, Section 203 directs the Secretary of Treasury to "develop procedures for the acceptance of signatures in digital or other electronic form." No particular technology is prescribed nor are the terms electronic or digital signatures defined. However, the legislation does provide that an electronic signature shall have the same effect as a manual signature for criminal and civil purposes. In addition, it states that an electronic signature "shall be presumed to have been actually submitted and subscribed by the person on whose behalf it was submitted." The bill creates a rebuttable presumption that a form submitted with an electronic signature has been assented to by the signer. House Report No. 105-364 reveals that this is a new presumption that does not apply to manual signatures and that the IRS will establish procedures for the rebuttal of the presumption. H.R. 2676 passed the House on November 5, 1997 and was referred to the Senate Finance Committee on January 28, 1998. The Finance Committee has yet to decide if the rebuttable presumption will survive in the Senate version.

On November 8, 1997, Representative Baker (R-LA) introduced H.R. 2937, entitled the Electronic Financial Services Efficiency Act of 1997. This is the only bill that would apply to government and private transactions. Federal communications with digital signatures would be permitted. A new National Association of Certification Authorities would be created. As a mixed private and public body, it would share regulatory responsibilities with the Secretary of the Treasury. Electronic signatures would be permitted for all other communications unless prohibited by state law, provided the signature reliably establishes (1) that identity is correct and (2) that the subject matter has not been altered. Statutory approved technologies include PKI-styled digital signatures and signature dynamics. New technologies may be approved provided they meet criteria styled after California approach. Approved electronic authentication technologies would meet manual signature and writing requirements.

On November 11, 1997, Representative Eschoo (D-CA) introduced H.R. 2991, entitled the Electronic Commerce Enhancement Act of 1997. This is a limited transactional statute that permits electronic submissions for the filing of forms and accompanying signatures with the federal government. The bill utilizes a broad definition

of electronic signature that is representative of a enabling-styled statute but also recognizes a role for certification authorities and private party accreditation. Liability for certification authorities would be based on commercially reasonable standards. Government and private parties would be authorized to serve as certification authorities.

Finally, on February 2, 1998, Senator Bennett (R-UT) introduced S. 1594, entitled the Digital Signature & Electronic Authentication Law (SEAL) of 1998. A companion bill, H.R. 3472, was introduced in the House by Representative Cook (R-UT) on March 17, 1998. The SEAL bill would permit the use of "electronic authentication" by financial institutions if the financial institution (1) agreed to use electronic authentication with another party or (2) had established a banking, financial, or transactions system that uses electronic authentication. Cryptographic and other secure electronic methods would be permitted provided the method allowed the user to (1) authenticate the identity of or information associated with a sender of a document; (2) determine that a document was not altered; or (3) verify that a document received was sent by the identified party claiming to be the sender. State regulators would be preempted from regulating electronic authentication by financial institutions.

C. Conclusions

The findings of this update support the conclusions of the initial ILPF survey. There is still no uniformity among the states' approaches to electronic authentication. However, it is apparent is that the comprehensive prescriptive approach characterized by Utah's statutory and regulatory scheme is no longer leading the way and may be, in fact, disfavored. The trend in the law is toward technology-neutral statutes that afford other new and existing technologies some means of equivalent recognition. Finally, standards for cross-border recognition continue to be largely ignored in all but the prescriptive initiatives, and even those provisions pose potential barriers to electronic commerce by not recognizing or giving lesser legal significance to electronic signatures made in other states.

The new federal initiatives are just as fragmented in their approach to electronic authentication as the states' initiatives. The fact that there is activity at the federal level with some hint of state preemption suggests that inconsistent state legislation is viewed as a significant threat to electronic commerce.

ILPF will continue to monitor these trends and periodically report on electronic authentication legislation.