

# THE ELECTRONIC SIGNATURE ACT OF 1996: BREAKING DOWN BARRIERS TO WIDESPREAD ELECTRONIC COMMERCE IN FLORIDA

WILLIAM E. WYROUGH, JR.\* AND RON KLEIN\*\*

I. INTRODUCTION .....	408
II. BACKGROUND .....	409
A. The Development of Electronic Commerce.....	409
1. What Is Electronic Commerce? .....	409
2. The Advantages of Electronic Commerce.....	410
3. The Federal Commitment to Electronic Commerce.....	410
4. Florida Moves Towards Electronic Commerce.....	411
a. Paperwork Reduction Efforts.....	411
i. Paperwork Reduction Act.....	411
ii. Paperwork Reduction Task Force.....	412
b. Examples of State and Local Government Initiatives.....	412
i. Florida Communities Network.....	412
ii. Department of State.....	413
iii. Florida State University's Purchasing System.....	413
iv. Department of Banking and Finance.....	413
v. Sarasota County Clerk of the Court.....	414
B. Security Issues in Electronic Commerce .....	414
1. Security in Closed Networks .....	414
2. Security in Open Networks and the Internet.....	414
3. Firewalls.....	416
4. Development of Modern Cryptography .....	416
a. Data Encryption Standard (DES).....	416
b. Escrowed Encryption Standard (EES).....	417
c. RSA Encryption.....	417
d. Government Control Efforts .....	418
III. ELECTRONIC COMMERCE AND THE LAW OF SIGNATURES.....	418
IV. DEVELOPMENT OF DIGITAL SIGNATURES .....	422
A. Private Key (Symmetric) Cryptography.....	422
B. Public Key (Asymmetric) Cryptography.....	423
1. Integrity, Authenticity, and Digital Signatures.....	424
2. Associating the Public Key with the Person .....	424
a. Pretty Good Privacy (PGP) "Web of Trust" Model.....	425
b. Certification Authorities and Public Key Certificates.....	426
D. Digital Signature Initiatives.....	427
1. Federal Government.....	427
2. Private Sector.....	428

---

\* Staff Attorney, Joint Committee on Information Technology Resources, Florida Legislature. B.A., University of Alabama, 1981; M.B.A., University of Alabama, 1983; J.D., Stetson University, 1990. As the staff attorney for the Joint Committee on Information Technology Resources, Mr. Wyrrough studied the topic of this Article and prepared a report based upon his findings. Those findings are the basis for this Article, and the authors have excerpted portions of the report into the Article. The views expressed in this Article are those of the authors and are not intended to reflect the opinion of the Florida Senate, the Florida House of Representatives, or the Joint Committee on Information Technology Resources.

\*\* Dem., Boca Raton, Florida Senate. B.A., The Ohio State University, 1979; J.D., Case Western Reserve University, 1982. Senator Klein is the former chair of the Joint Committee on Information Technology Resources.

3. Other States .....	429
a. Utah Legislation.....	429
b. California Legislation.....	430
c. Wyoming Legislation .....	431
d. State of Washington Legislation.....	432
4. American Bar Association Digital Signature Guidelines.....	432
V. THE JOINT COMMITTEE'S CONCLUSIONS AND RECOMMENDATIONS .....	432
A. Legal Status of Electronic Documents .....	432
B. The Legal Status of Electronic Signatures.....	433
C. Promoting the Use of Digital Signatures.....	433
D. Promoting Electronic Commerce in State Agencies.....	433
E. Future of Digital Signatures.....	434
VI. THE ELECTRONIC SIGNATURE ACT OF 1996.....	434
A. Legislative Intent.....	435
B. Definitions .....	435
C. The Legal Effect of Electronic Signatures.....	436
D. The Secretary of State as a Certification Authority for Digital Signatures .....	436
E. Accountability for Use of Electronic Commerce by State Agencies .....	437
F. Possible Future Role of the Secretary of State.....	437
VII. CONCLUSION.....	437

## I. INTRODUCTION

The current information revolution has seen an increasing number of people using computers to exchange all types of information.<sup>1</sup> The rapid proliferation of affordable hardware and software, as well as affordable network connections, is making it more practical for people from all walks of life to take advantage of information technology.<sup>2</sup> As a result, opportunities are being created to make information flow more efficiently and accurately between people.

Using computers and telecommunications to conduct business transactions is generally referred to as electronic commerce.<sup>3</sup> Electronic commerce makes it possible to replace paper forms and documents with their electronic equivalents for many types of activities.<sup>4</sup> Applications of electronic commerce can be found throughout the public and private sectors, including the practice of law.<sup>5</sup>

A major concern when making the transition from a paper-based commercial environment to an electronic system of commerce is the effect that replacing written signatures may have upon the reliability and legality of transactions.<sup>6</sup> New technologies are making it

---

1. See L.A. Lorek, *Internet Helps PC Users Become Well Connected* FT. LAUD. SUN SENT., May 16, 1994, at B7.

2. See *id.*

3. See Bruce Caldwell, *Bank Shot: Microsoft and Intuit Want to Help Banks Create the New World of Electronic Commerce* INTERNET WORLD, Dec. 18, 1995, at 14, 14.

4. See *id.*

5. See *id.*

6. See OFF. OF TECH. ASSESSMENT, U.S. CONGRESS, *INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 20-21* (1994).

possible to use electronic signatures to authenticate and preserve the integrity of transactions and documents.<sup>7</sup> For courts and lawyers, this means that the use of electronic pleadings, interrogatories, depositions, and briefs is becoming possible and practical.

In response to these developments, the Florida Legislature's Joint Committee on Information Technology Resources (Joint Committee) conducted an interim study of issues relating to electronic commerce and electronic signatures.<sup>8</sup> As a result of that study, the Joint Committee produced a report, with conclusions and recommendations, that became the basis of the Electronic Signature Act of 1996.<sup>9</sup>

This Article examines the issues associated with making the transition to electronic commerce via the use of electronic signatures and discusses the Electronic Signature Act of 1996. Part II discusses both electronic commerce and its concomitant security issues to provide a better understanding of the significance of electronic signatures. Part III discusses the history of traditional signatures and their legal importance, and provides a brief introduction to electronic signatures. Part IV examines the development of a type of electronic signature called a "digital signature." Part V highlights the conclusions and recommendations of the Joint Committee that formed the basis of the electronic signature legislation. Part VI describes the Electronic Signature Act of 1996, discusses its enactment, and analyzes its possible effect.

## II. BACKGROUND

### A. The Development of Electronic Commerce

#### 1. What Is Electronic Commerce?

Electronic commerce is a broad concept that, for the purposes of this Article, is defined as the use of computers and telecommunications to conduct business transactions.<sup>10</sup> These transactions include the placing and tracking of orders, the delivery of products and services, the exchange of funds, and the documentation of such events.<sup>11</sup> In addition, electronic commerce may involve electronic

---

7. See *id.* at 71-74 (arguing that the Uniform Commercial Code should be revised to include electronic signatures in the definition of "signed").

8. See FLA. LEGIS. JT. COMM. INFO. TECH. RESOURCES, ELECTRONIC SIGNATURES: A KEY TO UNLOCKING ELECTRONIC COMMERCE IN FLORIDA 1 (1996) [hereinafter ELECTRONIC SIGNATURES].

9. Ch. 96-224, 1996 Fla. Laws 837.

10. See Brian Miller, How to Sign on the Digital Line GOV'T TECH., June 1995, at 14, 14.

11. See *id.*

submission of various types of documents to government entities such as regulatory agencies and courts.<sup>12</sup>

One type of electronic commerce is electronic data interchange (EDI), which focuses on the electronic equivalent of paper forms such as purchase orders, shipping manifests, Medicaid claims, loan applications, and electronic benefits transfers.<sup>13</sup> EDI transactions typically conform to standards for formatting and sequencing data in electronic transmissions.<sup>14</sup>

## 2. The Advantages of Electronic Commerce

Electronic commerce reduces paperwork and improves the speed and accuracy of many processes in both the public and private sectors.<sup>15</sup> It improves the processing of many types of filings and transactions that take place between the government and private sector, such as tax returns, corporate filings, and legal memoranda.<sup>16</sup> An example is the Texas plan to automate the thousands of Uniform Commercial Code filings the state processes each year.<sup>17</sup> Advocates of the Texas plan estimate that automation will reduce the processing time of these filings from ten days to two minutes.<sup>18</sup>

The potential benefits to the private sector from electronic commerce are considerable.<sup>19</sup> On-line purchases and money transfers over telecommunications networks can have a significant impact on how business is conducted.<sup>20</sup> Securing deals and completing transactions quickly and accurately is critical for businesses to be competitive in the information age.<sup>21</sup>

## 3. The Federal Commitment to Electronic Commerce

The federal government has been actively pursuing goals related to furthering electronic commerce.<sup>22</sup> For example, on October 26, 1993, President Clinton issued a memorandum to the heads of all

12. See *id.*

13. See Bob Lynch, *Electronic Data Interchange: How to Begin GOV'T TECH.*, June 1995, at 40, 40.

14. See *id.*

15. See *id.*

16. See Blake Harris, *Electronic UCC Filing Faster and Cheaper GOV'T TECH.*, June 1995, at 1, 54.

17. See *id.* at 56.

18. See *id.* at 54.

19. See, e.g., *id.* at 1 (claiming that electronic UCC filing will save time, paperwork, and money).

20. See Roy E. Slagle & Paul A. Schaffman, *CFA Promotes EDI Tech*, *THE SECURED LENDER*, Oct. 1994, at 18, 21.

21. See *id.*

22. See President's Memorandum to the Heads of Executive Departments and Agencies on Streamlining Procurement Through Electronic Commerce, 29 *WEEKLY COMP. PRES. DOC.* 2174 (Nov. 1, 1993).

executive departments and agencies instructing them to implement electronic commerce in federal procurement procedures.<sup>23</sup> The President noted that electronic commerce would be cost effective and would simplify and streamline the purchasing process, promote customer service, and increase competition by improving access to federal contracting opportunities.<sup>24</sup> According to the memorandum, electronic commerce will fundamentally alter and improve the way the federal government buys goods and services.<sup>25</sup> Further, the memorandum included a time-line that called for complete government-wide electronic commerce for purchases, where possible, by January 1997.<sup>26</sup>

#### 4. Florida Moves Towards Electronic Commerce

Various efforts have been made to foster electronic commerce in Florida.<sup>27</sup> Efforts include initiatives taken by state government, local government, and Florida State University. These initiatives are highlighted below.

##### a. Paperwork Reduction Efforts

###### i. Paperwork Reduction Act

During the 1992 legislative session, chapter 282, Florida Statutes, was amended by the passage of the Information Resources Management and Paperwork Reduction Act.<sup>28</sup> The Act placed special emphasis on reducing the government's paperwork burden.<sup>29</sup> The amendments called for the specific reduction of paperwork associated with the collection and dissemination of government information to and from individuals, small businesses, educational institutions, state agencies, and local governments.<sup>30</sup> Agencies would achieve this reduction by reviewing, on a regular basis, their paperwork requirements, and devising plans to streamline their reports and forms.<sup>31</sup> The use of electronic commerce is consistent with the Paperwork Reduction Act's intent because it significantly reduces

---

23. See *id.*

24. See *id.*

25. See *id.*

26. See *id.* at 2175.

27. See ELECTRONIC SIGNATURES, *supra* note 8, at 22.

28. Ch. 92-98, 1992 Fla. Laws 870.

29. See FLA. STAT. § 282.004 (1995).

30. See *id.*

31. See *id.*

the amount of paperwork involved in doing business with the state of Florida.<sup>32</sup>

ii. Paperwork Reduction Task Force

On June 19, 1995, Governor Lawton Chiles signed an executive order establishing the Governor's Task Force on Paperwork Reduction.<sup>33</sup> One of the purposes of the Task Force is to promote an economic climate that supports the growth of business and efficient operation of government.<sup>34</sup> The Task Force's mission is thus consistent with the benefits derived from electronic commerce. Task Force members, however, found that the legal staffs of some agencies were uncertain about the legal standing of electronic documents and signatures.<sup>35</sup> The Task Force submitted recommendations in a report to the governor on January 31, 1996.<sup>36</sup>

b. Examples of State and Local Government Initiatives

i. Florida Communities Network

The Florida Communities Network is a new initiative by the Florida Department of Management Services that uses a statewide telecommunications network, SUNCOM. The network helps state agencies, cities, counties, and qualified nonprofit organizations provide information and services faster and more efficiently by establishing and linking various Florida World Wide Web sites on the Internet.<sup>37</sup> For example, through the Florida Communities Network, one can access information on state government job vacancies and contract purchasing opportunities, as well as information on many private sector companies.<sup>38</sup>

Information and links to other World Wide Web sites are regularly being added to the Florida Communities Network.<sup>39</sup> William H. Lindner, Secretary of the Department of Management Services, describes the Network as an "effort to establish Florida as a leader in economic development and government efficiency through electronic commerce."<sup>40</sup>

32. See Information Resources Management and Paperwork Reduction Act, ch. 92-98, § 2, 1992 Fla. Laws 870, 871 ("The state should minimize the paperwork burden associated with the collection and dissemination of government information for individuals, small businesses, educational institutions, state agencies, and local governments.").

33. See Fla. Exec. Order No. 95-215 (June 19, 1995).

34. See ELECTRONIC SIGNATURES, *supra* note 8, at 23.

35. See *id.*

36. See *id.* at 24; see also discussion *infra* Part V.

37. See ELECTRONIC SIGNATURES, *supra* note 8, at 24.

38. See *id.*

39. See *id.*

40. *Id.*

ii. Department of State

The Florida Department of State has implemented a system that allows electronic submission of UCC filings with the Division of Corporations.<sup>41</sup> After establishing an account with the Division, a user can file documents via fax.<sup>42</sup> Upon receipt by the Division, the original documents are electronically time-stamped and entered into the Division's UCC database.<sup>43</sup> Acknowledgment of accepted and rejected documents is returned to the originator via fax.<sup>44</sup>

The Division also has developed a public access system for corporate, UCC, and fictitious-names databases. The system provides network access to the databases via the CompuServe on-line service.<sup>45</sup>

iii. Florida State University's Purchasing System

The purchasing process at Florida State University has recently been automated with the inception of the General Requisition Electronic Entry and Tracking System (GREETs).<sup>46</sup> Before GREETs, university departments had to fill out requisition forms and obtain certain signatures throughout several layers of the approval process.<sup>47</sup> The requisition routing and budgetary approval processes are now paperless and completely automated.<sup>48</sup> Purchase orders, however, are still printed and signed.<sup>49</sup>

iv. Department of Banking and Finance

The Department of Banking and Finance's goal is to "develop a paperless, EDI-oriented computer system for processing 100 percent of the payment or disbursement requests received in the Comptroller's office."<sup>50</sup> One project directed by the legislature involves the electronic transfer of state funds to local governments.<sup>51</sup> Electronic transfers will reduce the number of paper warrants processed and significantly speed the transfer of those funds.<sup>52</sup>

---

41. See *id.*

42. See *id.*

43. See *id.* at 24-25.

44. See *id.* at 25.

45. See *id.*

46. See FLA. ST. UNIV. ADMIN. INFO. SYS., GENERAL REQUISITION ELECTRONIC ENTRY & TRACKING (GREETs VERSION 2.1) USERS GUIDE (1995).

47. See *id.* at 1.

48. See *id.*

49. See *id.* at 15.

50. Memorandum from Les Pearson, Chief, Fla. Bureau of Auditing, Office of the Comptroller, Dep't of Bank. & Fin. (Nov. 6, 1995) (on file with Fla. Legis. Jt. Comm. Info. Tech. Resources).

51. See FLA. STAT. § 17.076(6) (1995).

52. See ELECTRONIC SIGNATURES, *supra* note 8, at 27.

### v. Sarasota County Clerk of the Court

During the 1995 Regular Session, Representative Lisa Carlton<sup>53</sup> and Senator Katherine Harris<sup>54</sup> introduced House Bill 711<sup>55</sup> and Senate Bill 1770,<sup>56</sup> respectively. These bills would have provided an exception to the current law that requires a notary seal to be made with a rubber stamp.<sup>57</sup> The bills attempted to remove this requirement, which prevented the clerk of the court in Sarasota County from converting to a completely paperless process.<sup>58</sup> Certain documents in the court process require certified, or notarized, signatures. The bills would have allowed an electronic version of a notary seal.<sup>59</sup> The death of both bills in committee led to the Joint Committee's project on electronic signatures.<sup>60</sup>

## B. Security Issues in Electronic Commerce

### 1. Security in Closed Networks

Before the advent of open computer systems and open networks like the Internet, the bulk of electronic data was kept in closed computer networks, with access to the data controlled by the system operator.<sup>61</sup> Security for such networks was usually based upon a process through which each user was issued a user identification (ID), usually the user's name, and a password that the user entered.<sup>62</sup> Depending upon the user's need to access specific application programs, the system operator could control security by assigning different levels of access to each user ID.<sup>63</sup>

### 2. Security in Open Networks and the Internet

Because computing environments have become more decentralized and computers are being used more frequently for communicating and disseminating information, the security of the programs and data within computers is a greater concern.<sup>64</sup> Society is rapidly advancing toward the day when information technologies will be an integral part of daily life. Information networks are providing more

---

53. Repub., Osprey.

54. Repub., Sarasota.

55. Fla. HB 711 (1995).

56. Fla. SB 1770 (1995).

57. See FLA. STAT. § 117.05(3)(a) (1995).

58. See ELECTRONIC SIGNATURES, *supra* note 8, at 27.

59. See *id.* at 27-28.

60. See *id.* at 28.

61. See *id.*

62. See *id.*

63. See *id.*

64. See *id.*

people with access for many types of new uses. For example, efforts to bring electronic banking and "digital cash" or "digital checks" into homes and offices will have a great impact in the future.<sup>65</sup>

The chances of fraud and unauthorized access increase as more people use networked computers.<sup>66</sup> These problems become more prevalent when networks like the Internet are open to the public, as opposed to when networks are closed, access is strictly controlled, and security is primarily the concern of system administrators and security specialists. Thus, security is a concern for all users of computers linked to open networks.<sup>67</sup>

The Internet is a completely open network, with millions of users from all over the world on-line everyday.<sup>68</sup> Anyone with the right equipment and knowledge can use the Internet. As a result, hackers, thieves, con artists, and spies who are trying to covertly gather information for military, political, industrial, or personal advantage have easy access.<sup>69</sup> An attempt to break a security code is called an "attack," and the variety of attacks is limited only by the imagination of the attacker.<sup>70</sup>

Hackers can randomly generate computer IDs and passwords and access systems with relative ease.<sup>71</sup> In a test of a password generator called "Crack," more than thirty percent of one company's passwords were disclosed in less than a minute.<sup>72</sup> This lack of security has been cited as the main reason not to use the Internet for electronic commerce.<sup>73</sup> Depending upon the network environment, however, computer IDs and passwords may, in many cases, provide adequate security for a particular application.<sup>74</sup>

Although security was not a priority when the Internet was first created, the recent commercial interest in the Internet has spurred efforts to make transactions over the network more secure.<sup>75</sup> The basic connection protocol of the Internet, Terminal Control Protocol/Internet Protocol (TCP/IP), is undergoing a fundamental redesi-

---

65. See OFF. OF TECH. ASSESSMENT, U.S. CONGRESS, *ISSUE UPDATE ON INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 1-5* (1995) [hereinafter *OTA UPDATE*].

66. See, e.g., John Markoff, *Discovery of Internet Flaws Is Setback for On-Line Trade* N.Y. TIMES, Oct. 11, 1995, at A1 (stating that flaws in the Internet could allow easy access to confidential documents).

67. See *id.*

68. See *id.* at C3.

69. See, e.g., *id.* at A1 (arguing that flaws in the Internet could allow an eavesdropper or criminal to divert many documents).

70. See Lou Latham, *Network Security, Part 4: The Science of Encryption* INSIDE GARTNER GROUP THIS WK., May 17, 1995, at 16, 18-19.

71. See *id.*

72. See *id.* at 18.

73. Edward Yonkers, *Electronic Commerce on the Internet* INSIDE GARTNER GROUP THIS WK., July 26, 1995, at 1, 6.

74. See *id.*

75. See Markoff, *supra* note 66, at C3.

ign. A new protocol, called IP version six, will include special security features such as encryption and authentication, both of which are transparent to the user.<sup>76</sup>

### 3. Firewalls

The risks of unprotected communications over the Internet has led to a thriving business in creating Internet "firewalls," combinations of hardware and software that restrict access and filter data entering and leaving the network.<sup>77</sup> Firewalls can be installed in a variety of configurations and are available from many vendors.<sup>78</sup> Firewalls are limited, however, and must be implemented carefully and integrated with a total plan for security.<sup>79</sup> Firewall technology is not infallible; constant vigilance and frequent updating of security plans are essential for organizations linked to the Internet to ensure the integrity of the organization's data.<sup>80</sup>

### 4. Development of Modern Cryptography

Cryptography is a security tool that involves the ciphering and deciphering of a secret code.<sup>81</sup> In an environment using cryptography, people who have access to the plain data behind the scrambled data share a common key.<sup>82</sup> This key is a predetermined algorithm for use in ciphering and deciphering.<sup>83</sup> Cryptography has existed for centuries and has been especially useful during wartime; the use of modern, computer-based cryptography began during the World War II era.<sup>84</sup>

#### a. Data Encryption Standard (DES)

In 1977, the federal government adopted the Data Encryption Standard (DES) as a Federal Information Processing Standard (FIPS).<sup>85</sup> All executive branch agencies must use DES whenever cryptographic protection is needed for nonclassified data.<sup>86</sup> Outside

76. See *id.*

77. See Lou Latham, *Network Security, Part 3: Firewalls Bar the Door* INSIDE GARTNER GROUP THIS WK., May 10, 1995, at 11-12.

78. See *id.*

79. See *id.*

80. See *id.*

81. See OTA UPDATE, *supra* note 65, at 5.

82. See *id.*

83. See *id.*

84. See *id.*

85. See Edward J. Radio, *Legal Issues in Cryptography* COMPUTER LAW., May 1996, at 1, 2.

86. See A. Michael Fromkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution* 143 U. PA. L. REV. 709, 769 n.241 (1995). Prior to the adoption

the executive branch, however, the use of DES is voluntary and is only required for those who wish to exchange encrypted data with federal agencies.<sup>87</sup> DES is used extensively for transferring funds and communicating with the Federal Reserve System.<sup>88</sup>

#### b. Escrowed Encryption Standard (EES)

As the use of encryption technology in data communications increases, law enforcement agencies will face more difficulty when intercepting and decrypting electronic messages.<sup>89</sup> The federal government has responded to this potential loss of electronic surveillance ability by adopting the controversial Escrowed Encryption Standard (EES), also known as the "Clipper Chip."<sup>90</sup> With EES, law enforcement agencies can access an escrowed key that gives them the ability to unscramble data.<sup>91</sup> This ability, which allows the government to eavesdrop on confidential communications, is controversial because the federal government developed EES secretly and then promoted it as a standard.<sup>92</sup> Federal standards are usually developed with broad public input.<sup>93</sup>

The federal government is still developing its policy on escrow.<sup>94</sup> The Clinton Administration has created an Interagency Working Group on Encryption Policy and has issued a new Key Management Infrastructure proposal that would be voluntary for private industry.<sup>95</sup> However, this new proposal, which has been dubbed "Clipper II," has already come under sharp criticism.<sup>96</sup>

#### c. RSA Encryption

Today, the business community is more involved in electronic commerce, and thus its need for secure communications is driving the data security movement.<sup>97</sup> One company in particular, RSA Data

---

of the Escrowed Encryption Standard, see discussion *infra* Part II.B.4.b, federal agencies were required to use DES for sensitive, nonclassified data unless they procured a waiver. See Froomkin, *supra*, at 769 n.241.

87. See ELECTRONIC SIGNATURES, *supra* note 8, at 33.

88. See Karen E. Gegner & Stacy B. Veeder, Standards Setting and Federal Information Policy: The Escrowed Encryption Standard (EES) 11 GOV'T INFO. Q. 407, 407 (1994).

89. See ELECTRONIC SIGNATURES, *supra* note 8, at 33-34.

90. See Encryption Plan Ripped INFO. WK., Sept. 25, 1995, at 102.

91. See *id.*

92. See *id.*

93. See *id.*

94. See Kevin Power, Council Tells Administration to Back off Its Encryption Policy, GOV'T COMPUTER NEWS, June 10, 1996, at 3.

95. See *id.*

96. See *id.*

97. See ELECTRONIC SIGNATURES, *supra* note 8, at 34.

Security, Inc., has profited from this movement.<sup>98</sup> In 1977, the three founders of RSA developed and later patented an encryption algorithm that is now the de facto standard for commercial use.<sup>99</sup> RSA's Public Key Cryptosystem withstood tests by security experts and may be virtually impenetrable using existing, reasonably available technology.<sup>100</sup> The RSA algorithm has been incorporated into various companies' products, such as Lotus Notes and Netscape Navigator.<sup>101</sup>

#### d. Government Control Efforts

Through the Arms Control Export Act of 1976,<sup>102</sup> the federal government has attempted to control the export of strong encryption technologies, including those developed by RSA and others.<sup>103</sup> Export controls are an attempt to prevent strong encryption technology from being exported and possibly used in actions detrimental to national security.<sup>104</sup> Widespread foreign use of strong cryptography makes U.S. intelligence efforts more difficult because encrypted messages are hard to intercept and interpret.<sup>105</sup> Nevertheless, this export control policy has been criticized because it impairs the development of commercial encryption products.<sup>106</sup>

### III. ELECTRONIC COMMERCE AND THE LAW OF SIGNATURES

Traditionally, paper documents, signatures, and seals have been used to authenticate transactions and activities.<sup>107</sup> A certified notary public often added a further degree of reliability by authenticating the identity of the person signing a document.<sup>108</sup> These forms of authentication were typically used to meet the signature requirement in the statute of frauds.<sup>109</sup> This 300-year-old British statute is incorporated into Florida's version of the UCC and provides that certain contracts or engagements will not be enforceable by way of ac-

---

98. See Willie Schatz, *The Secret to Encryption: RSA Created a Security Code So Tough to Break, Leading Vendors Use It in Their Products* INFO. WK., May 15, 1995, at 74.

99. See *id.*

100. See *id.*

101. See *id.* at 76.

102. 22 U.S.C. § 2778 (1994).

103. See Schatz, *supra* note 98, at 74.

104. See *id.*

105. See ELECTRONIC SIGNATURES, *supra* note 8, at 35.

106. See Esther C. Roditti & Anne Fontaine, *Student Challenges Ban on Export of Encryption*, COMPUTER LAW & TAX REP., Apr. 1994, at 4-6. In addition, several bills are pending in Congress to change the current federal policies on encryption. See, e.g., *Encrypting Communications Privacy Act*, S. 1587, 104th Cong. (1996).

107. INFO. SECURITY COMM., ABA SCI. & TECH. SEC., DIGITAL SIGNATURE GUIDELINES 4-5 (1996) [hereinafter ABA GUIDELINES].

108. See *id.* at 31.

109. See *id.* at 82-84.

tion or defense unless there is some writing sufficient to indicate that a contract has been made between the parties and signed either by the party to be charged or by his or her authorized agent.<sup>110</sup>

The requirement for certain contracts to be in written form and signed has led to misunderstandings about the legality of electronic documents. By custom, the term "signature" has come to mean the name of a person written by that person at the end of the document, i.e., the person's autograph.<sup>111</sup> With this type of handwritten signature, one can use forensics to determine the authenticity of a signature.<sup>112</sup> Some believe that electronic documents should not be relied upon as legal documents because they do not contain such forensic evidence.<sup>113</sup> However, this historic view of a signature seems too narrow in a world undergoing rapid changes in technology.<sup>114</sup>

The UCC incorporates the statute of frauds by providing that many types of contracts are unenforceable without a "writing signed by the party against whom enforcement is sought."<sup>115</sup> Further, the UCC contains a general definition of the term "writing" that includes "printing, typewriting or any other intentional reduction to tangible form."<sup>116</sup>

This definition is inadequate for electronic documents. For example, does the phrase "tangible form" include computer hardware and software? In response to these questions, efforts are underway to revise the UCC to make it more relevant to a computerized environment.<sup>117</sup> One such effort proposes a new UCC Article 2B, concerning licenses.<sup>118</sup> Draft Article 2B replaces the term "writing" with "record," which it defines 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."<sup>119</sup>

In addition to the current UCC definition, section 1.01(4), Florida Statutes, contains a more general definition of the term "writing."<sup>120</sup> This general definition raises many of the same types of questions as the UCC definition when electronic documents are considered as writings.

---

110. See FLA. STAT. § 672.201(1) (1995).

111. See *Williams v. Dewey*, 178 N.E.2d 808, 809 (Ohio 1961).

112. See ELECTRONIC SIGNATURES, *supra* note 8, at 14 (noting that a handwriting expert can be called upon to give an opinion on the authenticity of a given signature).

113. See Benjamin Wright, *Contracts Without Paper*, TECH. REV., July 1992, at 57-58.

114. See ELECTRONIC SIGNATURES, *supra* note 8, at 14-15.

115. U.C.C. § 2-201(1).

116. *Id.* § 1-201(46).

117. See NAT'L CONF. OF COMM'RS ON UNIF. ST. LAWS, U.C.C. ART. 2B, LICENSES (draft of Sept. 4, 1996).

118. See *id.*

119. *Id.*

120. "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." FLA. STAT. § 1.01(4) (1995).

The UCC has broadly defined what will suffice for a signature. As defined in the Florida Statutes version of the UCC, the term "signed" includes "any symbol executed or adopted by a party with present intention to authenticate a writing."<sup>121</sup> For authentication, a complete signature is not necessary.<sup>122</sup> "Authentication may be printed, stamped or written; it may be by initials or by thumbprint. It may be on any part of the document and in appropriate cases may be found in a billhead or letterhead."<sup>123</sup> Courts have to rely upon "common sense and commercial experience" when determining if a signature is legally binding.<sup>124</sup>

The UCC's broad definition is consistent with the case law dealing with signatures.<sup>125</sup> A signature is not limited to an individual manually signing his or her full name on a contract. Rather, a signature is a "name, mark, or sign affixed to, or made on a document in token of knowledge, approval, acceptance, or obligation."<sup>126</sup> In the absence of a statute providing otherwise, a signature may be in one's handwriting, printed, stamped, typewritten, engraved, photographed, lithographed, or cut from one instrument and attached to another.<sup>127</sup> It is immaterial what type of instrument produces the signature.<sup>128</sup> An individual's initials also may be binding.<sup>129</sup> Additionally, a signature may be legally binding on a party if made by an individual acting as an agent for that party.<sup>130</sup> Further, absent a requirement that a signature appear in a particular place, a signature is not confined to a certain location on the instrument, but can be binding if signed anywhere on the instrument or attached to the instrument.<sup>131</sup> As long as a signature is affixed to a contract with the intention of authenticating and being bound by the writing, the signer is bound.<sup>132</sup> In sum, the signer's intent, not the signature's form, is what controls the legality of a signature.

In today's technological world, strict adherence to signatures on paper has become an archaic rule of law.<sup>133</sup> Although Florida law has never dealt with the concept of modern electronic signatures, some existing statutes are relevant. For example, section 15.16(4), Florida

---

121. *Id.* § 671.201(39).

122. See UCC § 1-201 official cmt. 39.

123. *Id.*

124. *Id.*

125. See, e.g., *State v. Hickman*, 189 So. 2d 254, 258 (Fla. 2d DCA 1966).

126. See 80 C.J.S. Signatures § 1(a) (1953).

127. See *Hickman*, 189 So. 2d at 258.

128. See *id.*

129. See *Gendzier v. Bielecki*, 97 So. 2d 604, 607 (Fla. 1957).

130. See *Hickman*, 189 So. 2d. at 258.

131. See *State v. Morris*, 223 So. 2d 743, 745 (Fla. 4th DCA 1969).

132. See 80 C.J.S. Signatures § 1(c) (1953).

133. Cf. ABA GUIDELINES, *supra* note 107, at 5 (suggesting that documents are written on paper today merely to satisfy the need for a legally recognized form).

Statutes, pertaining to the Department of State, states: "Notwithstanding any other provision of law, the department may certify or acknowledge and electronically transmit any record maintained by it."<sup>134</sup> This section recognizes the electronic transmission of official documents, but does not specifically address the issue of signatures. Further, section 116.34(3), Florida Statutes, states: "Any authorized officer, after filing with the Department of State his or her manual signature certified by him or her under oath, may execute or cause to be executed with a facsimile signature in lieu of a manual signature."<sup>135</sup> Some analogies to the use of electronic signatures can be drawn from this law because it departs from a strict adherence to manual signatures on a piece of paper. The statute also recognizes that validity and reliability can be achieved if the Department of State processes and keeps files of manual signatures to correspond with the facsimile signatures.<sup>136</sup>

In electronic commerce, traditional paper signatures can be replaced by using a variety of methods that are incorporated into the broad term "electronic signatures."<sup>137</sup> An electronic signature can be as simple as a signature on a document sent via fax.<sup>138</sup> It also can be a name or some other identifier included in an e-mail message.<sup>139</sup> Other forms of authentication may include the use of tokens such as smart cards.<sup>140</sup> Smart cards are similar in size and appearance to a traditional credit card.<sup>141</sup> A particularly secure type of electronic signature, known as a digital signature, is discussed in more detail below.<sup>142</sup>

A person's identity also may be associated with a message by using biometrics to analyze a person's unique physical attributes.<sup>143</sup> Attributes may include one's face, fingerprints, or retinas.<sup>144</sup> Another currently available technology performs a digital analysis of a person's written signature to verify authenticity.<sup>145</sup> Biometrics and other related technologies may be an appropriate authentication

---

134. FLA. STAT. § 15.16(4) (1995).

135. Id. § 116.34(3).

136. See id.

137. See ABA GUIDELINES, *supra* note 107, at 35.

138. Cf. id. (stating that electronic signatures include digitized images of paper-based signatures).

139. See id.

140. See id.

141. See id.

142. See discussion *infra* part IV.B.1.

143. See ABA GUIDELINES, *supra* note 107, at 7.

144. See id.

145. See Benjamin Wright, Eggs in Baskets: Distributing the Risks of Electronic Signatures, electronic copy available for purchase at <[http://www.infohaus.com/by-seller/access/Benjamin\\_Wright](http://www.infohaus.com/by-seller/access/Benjamin_Wright)> (on file with Fla. Legis. Jt. Comm. Info. Tech. Resources); Cynthia Morgan, Act of Signing Becomes Security Key, GOV'T COMPUTER NEWS, May 1, 1995, at 8.

solution for a given application; however, these types of authentication solutions usually require special hardware and added expense.<sup>146</sup>

Given that the concept of electronic signatures is relatively new, there is a lack of case law addressing the legality of electronic signatures. However, cases have upheld the legality of transactions with fax signatures as long as an intent to authenticate a writing is present.<sup>147</sup>

Identities and documents can be authenticated in many ways. One method may be more secure than another in a given situation. However, the law generally does not require that a signature be secure or fraud-proof to be legally effective.<sup>148</sup>

#### IV. DEVELOPMENT OF DIGITAL SIGNATURES

##### A. Private Key (Symmetric) Cryptography

Computers provide the ability to make cryptography algorithms more complex and difficult to decipher.<sup>149</sup> Messages and other data can be encrypted using a particular software program and then decrypted using the same or similar software.<sup>150</sup> In such cases, the encryption and decryption processes must share a common key.<sup>151</sup> This type of cryptographic security system is called a "private key" or "symmetric" cryptosystem.<sup>152</sup> The keys must be private to prevent unauthorized access to the confidential data.<sup>153</sup>

DES is currently the most commonly used private key system,<sup>154</sup> and is considered by experts to be relatively resistant to most forms of attack.<sup>155</sup> This system has been used extensively in military intelligence and financial environments.<sup>156</sup>

Private key cryptography is useful to ensure the security of computer systems and maintain confidentiality of information.<sup>157</sup> It also is useful as a means of authenticating the identities of people and documents in electronic commerce, provided the sender and the recipient have a preexisting relationship and there are tight controls

146. See ABA GUIDELINES, *supra* note 107, at 16-17.

147. See, e.g., *Parma Tile Mosaic & Marble Co. v. Estate of Short*, 663 N.E.2d 633 (N.Y. 1996).

148. See, e.g., *id.* at 635 & n.1 (noting that the court will look to the intent of the parties and accept a fax document as sufficient to constitute a writing).

149. See SIMON GARFINKEL, *PGP: PRETTY GOOD PRIVACY* 52-53 (1995).

150. See *id.* at 42.

151. See *id.*

152. See *id.*

153. See *id.*

154. See Latham, *supra* note 70, at 17.

155. See, e.g., GARFINKEL, *supra* note 149, at 43.

156. See *id.* at 45.

157. See OTA UPDATE, *supra* note 65, at 6.

on key distribution.<sup>158</sup> However, private key cryptography is not practical for secure communications between certain entities or between private citizens. Public uses are difficult because the sender and recipient must have the same key to encrypt and decrypt; they have to transmit the secret key between each other.<sup>159</sup> If open data networks are used to exchange the private keys, the possibility of compromise is greater.<sup>160</sup>

Another drawback of private key cryptography and DES is the inability to authenticate content.<sup>161</sup> There is no way to verify the actual content of the message, or whether it was secretly changed by either the sender or the recipient. A third person would be unable to identify who made the change because either party could have used the common secret key to forge the other party's name.<sup>162</sup>

### B. Public Key (Asymmetric) Cryptography

A major advance in cryptography came in the 1970s, when an alternative to private key cryptosystems was developed.<sup>163</sup> This system is called a "public key" or "asymmetric" cryptosystem.<sup>164</sup> Under this system, the sender and the recipient of electronic messages each use two mathematically generated keys, one public and one private.<sup>165</sup> The sender of a message locks or encrypts the data using the recipient's public key, which is made available to anyone.<sup>166</sup> Data in the message remains encrypted until it is decrypted by the intended recipient using his or her own private key.<sup>167</sup>

One advantage of public key cryptography over private key systems is that people who have never met can send encrypted electronic messages.<sup>168</sup> Further, public key cryptography resolves the private key cryptography problem of finding a secure way to exchange keys by eliminating the need to exchange them.<sup>169</sup> By pairing public and private keys together, "public key cryptography makes secure communications routine and potentially ubiquitous."<sup>170</sup>

---

158. See *id.*

159. See GARFINKEL, *supra* note 149, at 42, 45-46.

160. See *id.* at 46.

161. See *id.* at 55.

162. See *id.*

163. See *id.* at 49.

164. See *id.* at 48.

165. See *id.*

166. See *id.*

167. See *id.*

168. See *id.*

169. See *id.*

170. Latham, *supra* note 70, at 17.

## 1. Integrity, Authenticity, and Digital Signatures

Public key or asymmetric cryptography is one basis for digital signatures. A digital signature is defined as:

A transformation of a message using an hash function such that a person having the initial message and the signer's public key can accurately determine

(1) whether the transformation was created using the private key that corresponds to the signer's public key, and

(2) whether the initial message has been altered since the transformation was made.<sup>171</sup>

A digital signature, which is a form of electronic signature, can simultaneously authenticate a document's signer and check the document's integrity.<sup>172</sup> For electronic documents, a digital signature allows the recipient of the message to determine whether the message and the sender are authentic by using the sender's public key.<sup>173</sup> If the message was initially signed digitally using the private key of an individual sender, then the digital signature can only be verified by the recipient using the public key of the same individual sender.<sup>174</sup>

Digital signatures also may be used to verify message integrity.<sup>175</sup> To verify the integrity of a message, digital signature software uses a hash function to create a message digest, which is a number containing a mathematical summary that identifies the content of the message at the time the digital signature was created.<sup>176</sup> If the message is subsequently altered, the message digest cannot be matched by the recipient when the message is unscrambled and message integrity is lost.<sup>177</sup>

Another important aspect of digital signatures is that they do not allow repudiation if the sender denies sending the message.<sup>178</sup> Non-repudiation binds signers to statements, which can be extremely important in many types of transactions, especially when settling disputes.<sup>179</sup>

## 2. Associating the Public Key with the Person

A digital signature assures the recipient of a message that the sender's private key corresponds with the public key obtained by the

171. ABA GUIDELINES, *supra* note 107, at 35.

172. See GARFINKEL, *supra* note 149, at 12.

173. See Latham, *supra* note 70, at 18.

174. See *id.*

175. See *id.*

176. See *id.*

177. See *id.* at 18.

178. See *id.*

179. See *id.*

recipient.<sup>180</sup> Nevertheless, even this may not assure authenticity.<sup>181</sup> Even if the keys correspond with each other mathematically, there is no intrinsic association with a particular person.<sup>182</sup> In some cases, this association can be made using other available evidence.<sup>183</sup> For example, if two remote parties are attempting to conduct business using digital signatures to verify documents, one party may not be willing to take the other party's word that he or she is the person identified with a particular key pair. There is a risk that an impostor may be attempting to conduct the transaction.<sup>184</sup> The solution to this problem is to have one or more third parties, trusted by both of the original parties, certify the real people associated with the key pairs.<sup>185</sup>

a. Pretty Good Privacy (PGP) "Web of Trust" Model

Pretty Good Privacy (PGP) is a computer program that performs public-key cryptography, private key cryptography, and key management.<sup>186</sup> It is considered a very secure encryption method and is available on the Internet at no cost.<sup>187</sup>

The recipient of a message with PGP receives the public key of the sender along with the message, and thus can transform and decrypt the message.<sup>188</sup> The receiver must then judge whether the public key used is actually associated with the person identified as the sender.<sup>189</sup> To do this, the recipient may verify the public key with another trusted person.<sup>190</sup> That third party can say he or she knows and trusts the sender and the public key, thereby adding some measure of reliability to the process.<sup>191</sup> Such verifications can be repeated as often as necessary. This scheme has come to be known as the PGP "Web of Trust."<sup>192</sup>

---

180. See GARFINKEL, *supra* note 149, at 39.

181. See *id.* at 39-42.

182. Cf. *id.* (explaining that cryptography cannot protect against stolen encryption keys).

183. See *id.*

184. Cf. *id.* (explaining that any attacker who can steal or purchase your keys can decrypt your files and messages).

185. See ABA GUIDELINES, *supra* note 107, at 7.

186. See GARFINKEL, *supra* note 149, at 53.

187. See *id.* at 53, 379. PGP can be obtained by filling out a required form at PGP Distribution Authorization Form (visited Dec. 24, 1996) <<http://bs.mit.edu:8001/pgp-form.html>>.

188. See *id.* at 233.

189. See *id.*

190. See *id.* at 235-36.

191. See *id.*

192. See *id.*

## b. Certification Authorities and Public Key Certificates

Another solution to the problem of associating the public key with the person involves the use of certification authorities.<sup>193</sup> A certification authority issues a public key certificate to associate a person with a key pair.<sup>194</sup> Publication of these certificates in a repository makes a public key and its identification with a specific subscriber accessible to anyone seeking to verify a digital signature.<sup>195</sup> Repositories are kept in computer databases that the public can access remotely.<sup>196</sup> Further, such access can be accomplished automatically by the software used to verify digital signatures.<sup>197</sup> Therefore, the certificate identifies a key pair with a prospective signer or “subscriber” and gives a person verifying the digital signature the assurance that the public key corresponds with the person listed on the certificate.<sup>198</sup>

The certification authority also can digitally sign the certificate to assure authenticity.<sup>199</sup> The issuing certification authority’s digital signature on the certificate can be verified by checking the authority’s public key and certificate.<sup>200</sup> In this way, a matrix, or hierarchy, of certification authorities can be established to issue associated certificates.<sup>201</sup> A person verifying a digital signature can check the chain of associated certificates and certification authorities until he or she is adequately assured of its authenticity.<sup>202</sup>

Certification authorities can be either public or private entities.<sup>203</sup> Depending upon the circumstances, a subscriber could choose which certification authority meets his or her particular needs.<sup>204</sup> Certificates issued by a government certification authority may be perceived as the most trustworthy because the government is presumed to be acting in the public interest and is more stable than private entities.<sup>205</sup> On the other hand, a private entity may be more focused on critical tasks because its livelihood depends on its relationships with its customers.<sup>206</sup>

---

193. See ABA GUIDELINES, *supra* note 107, at 14-16.

194. See *id.* at 14.

195. See *id.* at 16.

196. See *id.*

197. See *id.*

198. See *id.* at 14-16.

199. See *id.* at 15.

200. See *id.*

201. See *id.*

202. See *id.*

203. See *id.* at 31.

204. Cf. *id.* at 60 (explaining that public policy or legislation may limit the extent to which the certification authority and subscriber may create enforceable agreements that are inconsistent with the fundamental principles of the Guidelines).

205. See ELECTRONIC SIGNATURES, *supra* note 8, at 43.

206. See *id.*

Certification authorities can be licensed by the government to issue certificates.<sup>207</sup> The license can therefore represent that the authority has met certain requirements, which gives that authority added credibility.<sup>208</sup> A scheme of licensing also can add standardization and uniformity to the widespread use of digital signatures.<sup>209</sup>

#### D. Digital Signature Initiatives

##### 1. Federal Government

The federal government has long been involved in the development and use of modern cryptography, primarily within the military and intelligence communities.<sup>210</sup> The National Institute of Standards and Technology, a part of the U.S. Department of Commerce, developed the Digital Signature Standard (DSS).<sup>211</sup> DSS was introduced in 1991 and approved as a Federal Information Processing Standard on May 19, 1994.<sup>212</sup>

DSS developers intended it to become the U.S. government's digital authentication standard.<sup>213</sup> Although DSS is the federal standard, the computer industry looks upon it unfavorably, preferring the RSA algorithm as a standard.<sup>214</sup> Unlike DSS, RSA can be used for secure exchanges of private keys.<sup>215</sup>

Public efforts to integrate digital signature technology include initiatives by the Internal Revenue Service (IRS), the U.S. Postal Service, and the General Services Administration (GSA). In 1995, the IRS announced plans to develop a signature verification scheme for income tax filings.<sup>216</sup> However, the IRS abandoned the plan because of disagreement over whether to use DSS or the more popular RSA.<sup>217</sup> The U.S. Postal Service is developing a system to certify electronic communications.<sup>218</sup> Under this system, the Postal Service would become a certification authority, certifying messages using

---

207. See *id.* at 45.

208. See *id.*

209. See *id.*

210. See *id.* at 20.

211. See GARFINKEL, *supra* note 149, at 138.

212. See Approval of Federal Information Processing Standards Publication 186, Digital Signature Standard (DSS), 59 Fed. Reg. 26,208, 26,208-09 (1994).

213. See GARFINKEL, *supra* note 149, at 138.

214. See *id.* at 138-39.

215. See *id.* at 57-58.

216. See Gary H. Anthes, Why You Didn't Cyberfile, COMPUTER WORLD, May 13, 1996, at 28, 28.

217. See *id.*

218. See James M. Smith, Mail No One Can Steam Open: Postal Service Will Lock Messages in Electronic Envelopes for Security, GOV'T COMPUTER NEWS, July 31, 1995, at 90, 90.

public key cryptography.<sup>219</sup> The GSA is developing a public key infrastructure for use by all federal agencies.<sup>220</sup> The GSA's planned infrastructure reportedly will incorporate RSA and DSS to allow use by both the government and private sector.<sup>221</sup>

## 2. Private Sector

The private sector has been involved in the use of digital signatures, especially for financial transactions.<sup>222</sup> RSA Data Security, Inc. invented the most commonly used algorithms and holds intellectual property rights to much of the technology used for public key cryptography.<sup>223</sup> In 1995, RSA formed VeriSign, Inc. to build a digital certificate infrastructure and to facilitate the use of digital signatures.<sup>224</sup> VeriSign is believed to be the first company devoted exclusively to issuing digital identification for electronic commerce.<sup>225</sup>

Visa and Mastercard have announced that they will jointly develop a safe way for customers to use their credit cards on the Internet.<sup>226</sup> The project will use encryption technology to create a common secure transaction standard.<sup>227</sup> Additionally, Wells Fargo Bank is working with Netscape Communications Corp. to develop a system to transfer encrypted information to its customers over the Internet.<sup>228</sup> Wells Fargo is the first bank to offer its customers access to account information over the Internet and plans to expand that service to include transactions.<sup>229</sup>

Further, the Bank of Boston, Bank of America, and Chemical Bank have become involved in forming the Financial Services Technology Consortium's electronic check project.<sup>230</sup> The consortium plans to use digital signatures to sign and endorse checks and digital certificates to authenticate electronic checks.<sup>231</sup>

---

219. See William Jackson, *Postal Service Gives Digital Signatures a Dry Run In-House*, GOV'T COMPUTER NEWS, Aug. 21, 1995, at 8, 8; Jill Gambon, *An On-line Post Office: Technology to Help Postal Service Get into Electronic Commerce* INFO. WK., May 1, 1995, at 28, 28.

220. See Kevin Power, *Digital Signatures: GSA Tosses a Hot Potato Back to NIST Lab* GOV'T COMPUTER NEWS, Oct. 2, 1995, at 1, 1.

221. See *id.* at 71.

222. See ELECTRONIC SIGNATURES, *supra* note 8, at 47.

223. See GARFINKEL, *supra* note 149, at 138.

224. See Ellis Booker, *Authentication Authority Formed to Check Digital IDs* COMPUTER WORLD, June 26, 1995, at 12, 12.

225. See *id.*

226. See Andrew Kantor & Tristan Louis, *The Internet: You Can Bank on It* INTERNET WORLD, Sept. 1995, at 12, 12.

227. See *id.*

228. See *id.*

229. See *id.*

230. See *id.*

231. See *id.*

### 3. Other States

Digital signature laws from other states provide sample frameworks for standardized digital signatures.<sup>232</sup> Utah, California, Wyoming, and Washington have enacted digital signature laws.<sup>233</sup> While the federal government had seemed poised to provide a model for a digital signature regimen, the prospects for such a model now appear slim.<sup>234</sup>

#### a. Utah Legislation

On March 9, 1995, Utah adopted digital signature legislation.<sup>235</sup> Repealed and reenacted in 1996,<sup>236</sup> the Utah Digital Signatures Act specifies four purposes for the liberal construction of the law:

- (1) to facilitate commerce by means of reliable electronic messages;
- (2) to minimize the incidence of forged digital signatures and fraud in electronic commerce;
- (3) to implement legally the general import of relevant standards . . . ; and
- (4) to establish, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages.<sup>237</sup>

The Act authorizes the licensing of certification authorities by the Division of Corporations and Commercial Code within the Utah Department of Commerce.<sup>238</sup> The Act allows multiple certification authorities, but specifies qualifications for licensure<sup>239</sup> and duties.<sup>240</sup> Prospective licensees must maintain detailed, computer-based records of issued certificates that identify subscribers, contain subscribers' public keys, and are digitally signed by the certification authority issuing the certificates.<sup>241</sup>

---

232. The ABA guidelines also offer a framework for digital signature laws. See discussion *infra* part IV.D.4.

233. See Digital Signatures Act, ch. 61, 1995 Utah Laws (WESTLAW) (codified as amended at UTAH CODE ANN. §§ 46-3-101 to -504 (Michie 1996)); Act of Sept. 5, 1995, ch. 594, 1995 Cal. Legis. Serv. (West, WESTLAW) (codified at CAL. GOV'T CODE § 16.5 (West 1995)); Act of Mar. 14, 1996, ch. 20, 1996 Wyo. Sess. Laws (WESTLAW) (to be codified at WYO. STAT. ANN. § 9-1-306); Act of Mar. 29, 1996, ch. 250, 1996 Wash. Legis. Serv. (West, WESTLAW).

234. See Kevin Power, Short of Cash, NIST Hands Off Its Digital Signature Program GOV'T COMPUTER NEWS, May 1, 1995, at 1, 1.

235. See Digital Signatures Act, ch. 61, 1995 Utah Laws (WESTLAW) (repealed and reenacted 1996).

236. See Digital Signatures Act, ch. 205, 1996 Utah Laws (WESTLAW).

237. UTAH CODE ANN. § 46-3-102 (Michie 1996).

238. See *id.* § 46-3-103(11), -3-201.

239. See *id.* § 46-3-201.

240. See *id.* § 46-3-301.

241. See *id.* § 46-3-103(3).

The Utah law is comprehensive and addresses many issues. These issues include: "(1) the responsibilities of certificate holders or 'subscribers'; (2) the liability of a licensed certification authority; and (3) the legal presumptions established by digital signatures."<sup>242</sup> One very significant presumption is that a digital signature has the same legal effect as a handwritten signature if certain requirements are met.<sup>243</sup> One of those requirements is that the digital signature be verified by reference to the public key listed in a valid certificate issued by a licensed certification authority.<sup>244</sup> This is controversial because it creates the inference that unless a digital signature meets all of the requirements it is not as valid as a signature on paper.<sup>245</sup> Essentially, the Act creates a higher standard for electronic signatures than is required for paper signatures.<sup>246</sup>

The Utah law lists the required contents of certificates issued by a licensed certification authority.<sup>247</sup> It also specifies the qualifications required to obtain or retain a license as a certification authority.<sup>248</sup> Further, the Act devotes a section to the duties of the certification authority and those of subscribers.<sup>249</sup> These duties are very specific and comprehensive.

The Act also addresses the liabilities of issuing certification authorities and accepting subscribers.<sup>250</sup> For example, the law states that by specifying "recommended reliance limits," certification authorities and subscribers recommend that persons should only rely upon the certificate in transactions in which the total amount of risk does not exceed the recommended reliance limit.<sup>251</sup> The law also states that a certification authority is not liable for losses due to forgeries, provided the authority complied with the law's requirements.<sup>252</sup>

## b. California Legislation

In California, digital signature legislation was enacted into law on September 5, 1995.<sup>253</sup> Unlike Utah's legislation, the scope of the

---

242. *Id.*

243. *See id.* § 46-3-401.

244. *See id.* § 46-3-401(1)(a).

245. *See* Benjamin Wright, *The Verdict on Plaintext Signatures: They're Legal* available for on-line purchase at <[http://infohaus.com/access/by-seller/Benjamin\\_Wright](http://infohaus.com/access/by-seller/Benjamin_Wright)> (on file with Fla. Legis. Jt. Comm. Info. Tech. Resources).

246. *See id.*

247. *See* UTAH CODE ANN. § 46-3-302 (Michie 1996).

248. *See id.* § 46-3-201.

249. *See id.* § 46-3-301.

250. *See id.* § 46-3-309.

251. *See id.* § 46-3-309(1)

252. *See id.* § 46-3-309(2).

253. *See* Act of Sept. 5, 1995, ch. 594, 1995 Cal. Legis. Serv. (West, WESTLAW) (codified at CAL. GOV'T CODE § 16.5 (West 1995)).

California law is limited to public sector transactions.<sup>254</sup> It enables parties who comply with the statutory requirements to conduct transactions with public entities by affixing digital signatures to related electronic documents.<sup>255</sup> The law states that the use of a digital signature has the same force and effect as the use of a manual signature only if it embodies certain specified attributes.<sup>256</sup>

Digital signatures are required to conform to regulations adopted by the California secretary of state.<sup>257</sup> By imposing conditions upon digital signatures, the California law creates a standard for electronic signatures that is arguably higher than the standard for written signatures. This concept, also embodied in the Utah law, is controversial because there arguably is no reason to have different standards for different forms of signatures. Further, requirements and conditions only serve to hamper the development of emerging digital signature technologies. However, the controversy is mitigated somewhat because California's law only applies to transactions involving the public sector.<sup>258</sup>

The California law rather broadly defines a digital signature as "an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature."<sup>259</sup> This definition does not include encryption.<sup>260</sup> Further, the law states that the use of digital signatures is optional.<sup>261</sup>

### c. Wyoming Legislation

During its 1995 session, the Wyoming Legislature passed a bill creating an electronic filing system law.<sup>262</sup> As amended in 1996,<sup>263</sup> the law authorizes Wyoming's secretary of state to develop a state-wide electronic filing system for required records.<sup>264</sup> The secretary is required to adopt rules to implement an electronic filing system if such a system is actually developed.<sup>265</sup> The rules must "prescribe a key encryption or other identification procedure for any person

---

254. See CAL. GOV'T CODE § 16.5(a) (West 1995).

255. See *id.*

256. See *id.*

257. See *id.* § 16.5(a)(5).

258. See *id.*

259. *Id.* § 16.5(d).

260. See *id.*

261. See *id.*

262. Act of Feb. 23, 1995, ch. 125, 1995 Wyo. Sess. Laws (WESTLAW) (codified as amended at WYO. STAT. ANN. § 9-1-306 (Michie 1996)).

263. Act of Mar. 14, 1996, ch. 20, 1996 Wyo. Sess. Laws (WESTLAW) (codified at WYO. STAT. ANN. § 9-1-306 (Michie 1996)).

264. See WYO. STAT. ANN. § 9-1-306 (Michie 1996).

265. See *id.* § 9-1-306(a)-(b).

wishing to file records or other documents,"<sup>266</sup> and "prescribe a procedure for certification of the electronic filings by the secretary of state."<sup>267</sup> The law also limits the liability of the secretary of state for problems arising from entry errors in the electronic filing system.<sup>268</sup>

#### d. State of Washington Legislation

On March 2, 1996, the state of Washington passed the Washington Electronic Authentication Act.<sup>269</sup> It is substantially similar to the Utah digital signature legislation.<sup>270</sup> The Washington Act becomes effective on January 1, 1998.<sup>271</sup>

#### 4. American Bar Association Digital Signature Guidelines

The American Bar Association has been involved in the development of model guidelines on digital signatures through the work of the ABA Science and Technology Section's Information Security Committee.<sup>272</sup> The guidelines were published on August 1, 1996.<sup>273</sup> The committee worked in close cooperation with Utah, and the guidelines are generally consistent with the Utah law.<sup>274</sup>

### V. THE JOINT COMMITTEE'S CONCLUSIONS AND RECOMMENDATIONS

#### A. Legal Status of Electronic Documents

Documents usually signed to show authenticity are termed "writings" for legal purposes.<sup>275</sup> The Joint Committee concluded, however, that the present definition of "writing" in section 1.01(4), Florida Statutes, is unclear as to whether documents in a digital or electronic medium are writings for the purposes of the law.<sup>276</sup> Therefore, the Joint Committee recommended that the Legislature amend the definition of "writing" to "include information which is created or stored in any electronic medium and which is retrievable in perceivable form."<sup>277</sup>

---

266. Id. § 9-1-306(b)(v).

267. Id. § 9-1-306(b)(vi).

268. See id. § 9-1-306(d).

269. Ch. 250, 1996 Wash. Legis. Serv. (West, WESTLAW).

270. See generally id.

271. See id. § 602.

272. See ABA GUIDELINES, *supra* note 107.

273. See id.

274. See DIV. OF CORP. AND COM. CODE, UTAH DEP'T OF COM., UTAH DIGITAL SIGNATURE LAW 1 (1995).

275. See 80 C.J.S. Signatures § 1(c) (1953).

276. See ELECTRONIC SIGNATURES, *supra* note 8, at 52 (citing FLA. STAT. § 1.01(4) (1995)).

277. Id.

### B. The Legal Status of Electronic Signatures

The Joint Committee concluded that Florida law does not presently preclude the use of electronic signatures.<sup>278</sup> Nevertheless, some entities may be reluctant to use them until the law gives such signatures the same force and effect as traditional signatures.<sup>279</sup> Additionally, the Joint Committee concluded that encouraging the transition to electronic commerce fosters the state's interests in economic development and in creating a more efficient and effective government.<sup>280</sup> The legal basis for the use of electronic signatures, including digital signatures, must be explicitly established.<sup>281</sup> The Joint Committee recommended that the Legislature amend the law to facilitate electronic commerce and the use of electronic signatures by stating that electronic signatures may be used to "sign" writings.<sup>282</sup>

### C. Promoting the Use of Digital Signatures

The Joint Committee studied the methods of authenticating signatures and documents that use digital signature technology.<sup>283</sup> It concluded that digital signatures are potentially more secure and efficient than manual signatures.<sup>284</sup> The Joint Committee also determined that state involvement in developing a legal infrastructure for third-party verification of digital signatures could enhance public trust and confidence in the use of digital signatures and thus benefit electronic commerce. Therefore, the Joint Committee recommended that the Legislature amend the law by allowing the secretary of state to serve as a certification authority.<sup>285</sup> The secretary would issue certificates verifying digital signatures and, when necessary, suspend or revoke certificates.<sup>286</sup>

### D. Promoting Electronic Commerce in State Agencies

The Joint Committee decided that digital signatures can be an effective way to authenticate electronic messages.<sup>287</sup> Easier mechanisms, however, also can be employed to add the appropriate level of security, authenticity, and integrity to electronic data used for elec-

---

278. See *id.*

279. See *id.*

280. See *id.*

281. See *id.*

282. See *id.* at 53.

283. See *id.*

284. See *id.*

285. See *id.*

286. See *id.*

287. See *id.*

tronic commerce. Such mechanisms include computer IDs, computer passwords, and facsimile technology.<sup>288</sup> The selection of the mechanism should depend upon the application's security risk.<sup>289</sup> The Joint Committee concluded that the use of any mechanism facilitating the transition to electronic commerce should be encouraged as a matter of public policy.<sup>290</sup> It recommended that state agencies review all agency rules and internal procedures that: (1) require paper formats; (2) limit the admissibility of electronic records based on their electronic character; (3) require handwritten signatures; or (4) require notarization that precludes electronic filings.<sup>291</sup> The Joint Committee recommended that agencies consider amending such rules and procedures based upon an assessment of security risks and impose functional, rather than format-specific, requirements.<sup>292</sup>

### E. Future of Digital Signatures

The Joint Committee concluded that the use of electronic commerce on the Internet is in its early stages.<sup>293</sup> Moreover, it found that it is not yet known whether electronic commerce in Florida requires certification authorities or a licensing system for certification authorities.<sup>294</sup> Comprehensive legislation on digital signatures requires additional study before it will be warranted in Florida. The Joint Committee thus encouraged the Legislature to require the secretary of state to study issues related to expanding the use of digital signatures for electronic commerce.<sup>295</sup> The secretary was to report the findings and recommendations to the Joint Committee by December 1, 1996.<sup>296</sup> The study should address whether additional legislation, such as a law establishing procedures for the public licensure of certification authorities and establishing legal presumptions for digital signatures, is required to further Florida electronic commerce.<sup>297</sup>

## VI. THE ELECTRONIC SIGNATURE ACT OF 1996

In response to the Joint Committee's report and recommendations, two bills were filed during the 1996 Regular Session. Senate

---

288. See *id.*

289. See *id.* at 53-54.

290. See *id.* at 54.

291. See *id.*

292. See *id.*

293. See *id.*

294. See *id.*

295. See *id.*

296. See *id.*

297. See *id.* at 54-55.

Bill 942<sup>298</sup> was sponsored by Senator Donald Sullivan,<sup>299</sup> while House Bill 1023,<sup>300</sup> an identical House companion, was sponsored by Representative (now Senator) Ron Klein.<sup>301</sup> Senate Bill 942 was eventually enrolled and became law on May 25, 1996.<sup>302</sup>

#### A. Legislative Intent

Section 2 of the Act provides legislative intent.<sup>303</sup> The Act's basic intent is to promote the development of electronic commerce in the public and private sectors.<sup>304</sup> To achieve this purpose, electronic messages must be reliable and the public must have confidence in the use of electronic signatures.<sup>305</sup> A functioning electronic commerce system thus requires a framework that can support secure electronic transactions.

#### B. Definitions

Section 3 of the Act amends the definition of "writing" in section 1.01, Florida Statutes, to include "information which is created or stored in any electronic medium and retrievable in perceivable form."<sup>306</sup> The Act thus makes it clear that electronic messages and documents are legally equivalent to paper documents.

Section 4 of the Act defines the terms "certificate," "certification authority," "digital signature," and "electronic signature."<sup>307</sup> These terms are particularly relevant to authenticating electronic messages and documents. An "electronic signature" is defined broadly to include "any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing."<sup>308</sup> Because electronic documents do not have the same physical characteristics as paper documents, the definition includes a statement that a document is "electronically signed if an electronic signature is logically associated with the document."<sup>309</sup> Other terms defined in the bill refer to digital signatures and a framework of certificates and certification authorities to support their use.<sup>310</sup>

---

298. Fla. SB 942 (1996).

299. Repub., Seminole.

300. Fla. HB 1023 (1996).

301. Dem., Boca Raton.

302. Electronic Signature Act of 1996, ch. 96-224, 1996 Fla. Laws 837.

303. See id. § 2, 1996 Fla. Laws at 837.

304. See id.

305. See id. §2(1)-(2).

306. Id. § 3, 1996 Fla. Laws at 837 (amending FLA. STAT. § 101(4) (1995)).

307. Id. § 4, 1996 Fla. Laws at 837-38 (codified at FLA. STAT. § 282.72 (Supp. 1996)).

308. Id. § 4(4), 1996 Fla. Laws at 838 (codified at FLA. STAT. § 282.72(4) (Supp. 1996)).

309. Id.

310. See id. § 4(1)-(3) (codified at FLA. STAT. § 282.72(1)-(3) (Supp. 1996)).

### C. The Legal Effect of Electronic Signatures

Section 5 of the Act states that use of electronic signatures is generally allowed under the law and gives electronic signatures the same force and effect as written signatures.<sup>311</sup> This is a clear departure from the Utah, California, and Washington acts, which only address digital signatures.<sup>312</sup> Conversely, the Florida law defines and distinguishes between the very broad term “electronic signature” and the more narrow term “digital signature.”<sup>313</sup> It gives electronic signatures the same force and effect as written signatures, unless otherwise provided by law.<sup>314</sup> Therefore, all types of existing and future electronic signatures, including digital signatures, are now generally on an equal legal footing with written signatures in Florida.

The Act does not address how secure electronic signatures must be to be legally effective. There may be cases where, for various reasons, agency regulations or court rules will specify exactly how signatures are to be made. However, for general purposes, the new language added by section 5 makes it clear that electronic signatures can be used for the same purposes, and have the same force and effect, as traditional signatures.<sup>315</sup>

### D. The Secretary of State as a Certification Authority for Digital Signatures

Section 6 of the Act authorizes the secretary of state to facilitate the use of digital signatures by issuing, suspending, or revoking certificates used to verify digital signatures.<sup>316</sup> It also authorizes the secretary to take necessary actions to achieve the purposes of the Act.<sup>317</sup> Therefore, the secretary of state has the discretion to become a certification authority if necessary. The secretary’s role as a certification authority would thus be to associate people with digital signatures for authentication purposes. This role, however, does not include any type of authority over, or regulation of, any other entity that chooses to be a certification authority in Florida.<sup>318</sup> Section 6 of the Act also authorizes the secretary to impose a fee for issuing a certificate, and requires the secretary to promulgate rules for certifi-

---

311. See *id.* § 5, 1996 Fla. Laws at 838 (codified at FLA. STAT. § 282.73 (Supp. 1996)).

312. See discussion *supra* Part IV.D.3.

313. Electronic Signature Act § 4(4), 1996 Fla. Laws at 838 (codified at FLA. STAT. § 282.72(4) (Supp. 1996)).

314. See *id.* § 5, 1996 Fla. Laws at 838 (codified at FLA. STAT. § 282.73 (Supp. 1996)).

315. See *id.*

316. See *id.* § 6, 1996 Fla. Laws at 838 (codified at FLA. STAT. § 282.74 (Supp. 1996)).

317. See *id.*

318. See *id.*

cation activities.<sup>319</sup> Any participation by the public or private sector in the secretary's certification program is voluntary.<sup>320</sup>

#### E. Accountability for Use of Electronic Commerce by State Agencies

Section 7 of the Act makes each agency head responsible for adopting certain control processes and procedures.<sup>321</sup> Such processes and procedures are intended to "ensure adequate integrity, security, confidentiality, and auditability of business transactions conducted using electronic commerce."<sup>322</sup> This section emphasizes the importance of addressing security issues in developing electronic commerce applications. Thus, accountability for security is placed with agency heads.

#### F. Possible Future Role of the Secretary of State

Section 8 of the Act directs the secretary of state to undertake a study of the issues related to expanding the use of digital signatures.<sup>323</sup> These issues include the secretary's role in promoting the use of digital signatures. In particular, the report is to address whether it is in the public interest for the secretary to (1) license, certify, or register certification authorities; (2) develop requirements for certification authorities to be licensed, certified, or registered; and (3) maintain a publicly accessible database that contains certification authorities.<sup>324</sup> The study also could cover topics such as standards for digital signatures, liability limits for certification authorities, and additional legislation and rules for digital signatures.<sup>325</sup> The findings of the study were reported to the Joint Committee on December 1, 1996.<sup>326</sup>

### VII. CONCLUSION

The development of widespread electronic commerce is a complicated process. Important developments must occur if people are to feel comfortable with changing the way they conduct business. Indeed, such developments are underway as society becomes accustomed to using computers and networks. This will lead to more effi-

---

319. See *id.*

320. "Nothing in this section shall be construed to compel any public or private entity to participate in the Secretary of State's certification program, as authorized in this section, in order to verify digital signatures." *Id.*

321. *Id.* § 7, 1996 Fla. Laws at 838 (codified at FLA. STAT. § 282.75 (Supp. 1996)).

322. *Id.*

323. See *id.* § 8, 1996 Fla. Laws at 838-39 .

324. See *id.*

325. See *id.*

326. See *id.*

cient networks and lower prices. Individual and networked applications are being developed to make it faster, easier, and safer to conduct electronic commerce.

Many people realize the potential of electronic commerce but are not yet demanding it. Such people are unlikely to use electronic signature software and hardware until they see that it is easy, beneficial, and legal. Leadership is needed in the private and public sectors to bring about change. The private sector must continue to develop and refine the networks, hardware, and software necessary to support electronic commerce. The public sector needs to facilitate electronic commerce by helping to build the processes and infrastructure, both operational and legal, to support secure and efficient electronic commerce.

The Florida Legislature took a leading role in the development of electronic commerce when it passed the Electronic Signature Act of 1996. The Legislature laid the basic legal foundation for treating electronic documents identically to other writings. Electronic signatures, including digital signatures, are defined in law and their legal effectiveness is established. Additionally, the secretary of state is involved in developing the infrastructure necessary to support reliable digital signatures. The Electronic Signature Act of 1996 is part of the process that will lead to widespread electronic commerce in the public and private sectors. To reap the benefits, however, the public and private sectors must work together to maximize the potential of electronic commerce.