Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*

I. INTRODUCTION

On March 9, 1995, the Utah Digital Signature Act (the "Utah Act") was signed into law.[1] Complex and ambitious, the Utah Act is intended to promote the use of digital signatures on computer-based documents and to facilitate electronic commerce.[2] The Utah Act implements an infrastructure in which computer users utilize "certification authorities," online databases called repositories, and public-key encryption technology in order to "sign" electronic documents in a legally binding fashion. In addition to setting out a regulatory scheme designed to implement this infrastructure, the Utah Act provides certain digital signatures with legal status as valid signatures and addresses a variety of issues relating to the status of digitally-signed electronic documents in contract and evidence law.

---

* B.A. University of California, San Diego; J.D. candidate, University of San Diego, May 1997. The author will be joining the San Diego office of Cooley Godward, LLP as an associate upon graduation. This Comment generally reflects developments through April 8, 1996. Special thanks to my wife Mare for all of her support. This comment is dedicated to our daughter Sophie, born February 5, 1996, with whom I spent many late nights pacing the floor and discussing the intricacies of public key cryptography.

1. The Utah Digital Signature Act was enacted by 1995 Utah S.B. 82, creating UTAH CODE ANN. §§ 46-3-101 to -504 (Supp. 1995). It was significantly amended by 1996 Utah S.B. 188, which repealed and reenacted large portions of the Act. The Act is found in its amended form at 1996 Utah Laws 46-3-101 to -502 (and will, when codified, add those sections to the Utah Code). When this Comment cites to a code section, it is referring to the 1996 amended version of the Act unless otherwise noted. An account of the history of the Utah Act can be found in DIVISION OF CORPORATIONS AND COMMERCIAL CODE, UTAH DEPARTMENT OF COMMERCE, UTAH DIGITAL SIGNATURE LAW: TECHNICALLY AND LEGALLY SECURE ELECTRONIC COMMERCE 17-18 (November 1995) (drafting committee's commentary to the now-enacted amended version of the Utah Act) [hereinafter UTAH DIGITAL SIGNATURE LAW].

2. § 46-3-102.

The potential benefits of the "public key infrastructure" implemented by the Utah Act are considerable. Conceivably, a well-functioning public key infrastructure could allow private individuals, businesses, and government to routinely and securely conduct personal, financial, and legal affairs over open networks like the Internet.[3] Legislation can potentially facilitate the development of this type of infrastructure. As the Utah Act illustrates, legislation can clarify the arguably uncertain legal status of digital signatures, determine liability standards in an emerging and unprecedented certification authority industry, clarify the rights and responsibilities of infrastructure participants, and address other important public policy concerns. In light of the significance of these issues, it is not surprising that more than ten states are following in Utah's footsteps and developing digital signature legislation.

As further described in Section IV of this Comment, the Utah Digital Signature Act has become a putative "Model Act" which other state legislatures are looking to when developing digital signature legislation. Thus, it is particularly important to recognize certain policy choices made by, and certain problems with, the Utah Act. This Comment analyzes one of these problem areas: the allocation of liability and evidentiary burdens.[4]

The drafters of the Utah Act made policy choices concerning liability allocation which are troubling. Consumers who participate in the infrastructure developed under the Utah Act subject themselves to a far greater risk of extensive liability than they face in a variety of analogous situations, and face difficult evidentiary burdens in resolving disputes that arise under the Act. Additionally, the financial responsibility provisions of the Utah Act create a *de facto* liability cap for one actor in the infrastructure, the certification authority, at an amount that could be significantly less than the actual damages a certification authority could cause.

---

3. For a general introduction to the Internet, see ED KROL, THE WHOLE INTERNET (1992). For a discussion of the advantages of the Internet over value-added networks (VANs) as a business tool, see Colleen Frye, *EDI Users Explore Internet as Tool of Trade*, SOFTWARE MAG., Dec. 1995, at 83 ("lower costs and more freedom are earning the 'Net a look as a vehicle for business commerce"). For a discussion of the *disadvantages* of the Internet relative to VANs, see BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE EDI E-MAIL AND THE INTERNET: TECHNOLOGY, PROOF, AND LIABILITY § ET1.3.5 (2d ed. 1995). *See also Internet Commerce Hung Up on Security*, EDI NEWS, Feb. 19, 1996, *available in* LEXIS, NEWS Library, ZTL1 File (noting that the Internet is "still daunting as a commercial vehicle" because of security concerns).

4. Some other criticisms of the Utah Act are surveyed in note 120, *infra*. A number of issues related to a public key infrastructure have recently been addressed in A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 U. OR. L. REV. 49 (1996).

This Comment begins by presenting a brief overview of digital signature technology in Section II (which can be skipped by those readers already familiar with basic cryptographic techniques without any significant loss of context). A summary of the Utah Digital Signature Act follows in Section III. Section IV describes the Utah Digital Signature Act's status as a putative "Model Act," and suggests that this status may not be entirely appropriate. In Section V, the focus turns to a comparison of the liability allocations and evidentiary burdens imposed by the Utah Act to three analogous models: the credit card model, the notary model, and the telecommunications toll fraud model. As part of the discussion of the credit card model, this Comment discusses the likely preemption of the Utah Act under certain limited circumstances by the consumer protection-oriented Electronic Fund Transfer Act.[5] An alternative approach to the apportionment of liability in a public key infrastructure is proposed, based upon a proposed reform in the analogous arena of telecommunications toll fraud. Ultimately this Comment asserts that the liability allocations of the Utah Act inappropriately impose potentially unlimited risk on users of digital signatures, ignoring an important policy of consumer protection. This Comment additionally asserts that the provisions of the Utah Act which limit the liability of certification authorities undermine the economic integrity of the infrastructure implemented by the Act. Lawmakers contemplating digital signature legislation should reconsider some of the policy choices made by the Utah Act.

II. DIGITAL SIGNATURES

Two preliminary observations are appropriate before exploring the technology behind digital signatures. First, digital signatures are not digital images of manually signed names. Rather, as further described below, the term describes a method of digital file encryption which facilitates verification of the integrity and authenticity of digital messages.[6]

---

5. 15 U.S.C. §§ 1693-1693r (1995).

6. Peter N. Weiss argues that the term "digital signature" is misleading in many ways, particularly because the term sparks the inference that legislation is necessary in order to accommodate the technology into the common law and statutory framework of written signatures. He notes that an awkward but more accurate description is "public key-based cryptographic originator authentication." E-mail message from Peter N. Weiss

Second, from a legal perspective, understanding the underlying technology of digital signatures is perhaps less important than understanding what using digital signatures can accomplish. If Alice "signs" an electronic document with a digital signature and sends it via electronic mail over the Internet to Bob, ideally Bob can be assured that, first, the document really came from Alice. Forging electronic mail messages on the Internet is easily accomplished. Digital signatures provide assurance that a message has in fact come from its purported sender. This assurance supplied by a digital signature is called "proof of origin" or "data origin authentication."[7] Second, Bob can be sure that the document he received is the exact document that Alice sent—it has not been altered since Alice sent it. A message sent over an open network like the Internet may pass through dozens of computer systems, each owned and operated by different entities. At every stage in this process the message is vulnerable to alteration. A digital signature enables a recipient to verify that a message has not been intentionally or accidentally altered, a quality known as "message integrity."[8] Third, Bob is assured that Alice cannot later deny that she sent the message (in order to avoid a promise that she made in the message, for example). No one but Alice could have sent the message, and Bob can prove it unequivocally. This quality of digital signatures is known as "non-repudiation."[9]

Achieving the three qualities of data origin authentication, message integrity, and non-repudiation requires the use of sophisticated cryptographic technology (which can be built into computer software or hardware) and the use of trusted third parties who can provide certain

---

to C. Bradford Biddle (February 23, 1996) (printed copy on file with author). *See generally* Peter N. Weiss, *Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Towards Developing a Security Policy*, 12 J. MARSHALL J. COMPUTER & INFO. L. 425 (1993).

7. Michael J. Ganley, *Digital Signatures and Their Uses*, 13 COMPUTERS & SECURITY 385 (1994). *See also* BRUCE SCHNEIER, E-MAIL SECURITY: HOW TO KEEP YOUR ELECTRONIC MESSAGES PRIVATE 98 (1995) [hereinafter SCHNEIER, E-MAIL SECURITY]. SCHNEIER, E-MAIL SECURITY is highly recommended as an excellent general introduction to the fundamentals of cryptography. Another excellent introduction to cryptography and digital signatures is Paul Fahn, *Answers to Frequently Asked Questions About Today's Cryptography*, published by RSA Laboratories, a division of RSA Data Security, on the Internet in a hypertext version at <http://www.rsa.com/rsalabs/faq/faq_home.html> and in an ASCII version at <http://www.rsa.com/pub/faq/faq.asc> (September 20, 1993) [hereinafter "RSA FAQ"]. This Comment cites to the section numbers of the RSA FAQ as presented in the ASCII version. A more sophisticated and comprehensive introduction to cryptography can be found in BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C (2d ed. 1996) [hereinafter SCHNEIER, APPLIED CRYPTOGRAPHY].

8. Ganley, *supra* note 7, at 385.

9. *Id.*

identification requirements and other services. The remainder of Section II discusses the mathematics and technology underlying digital signatures, and the institutional infrastructure that is necessary in order to make digital signatures work effectively.

A. Public Key Cryptography

Public key cryptography, developed in 1976, was a profound breakthrough in the science of cryptography.[10] Prior to the development of public key cryptography, cryptographers traditionally used secret key cryptography. Using secret key cryptography, both the sender and recipient of a message share the same secret piece of information, called a key, which is used in conjunction with an *algorithm* to both encrypt and decrypt (scramble and unscramble) the message.[11] Secret key cryptography is ill-suited for communications over open computer networks, because of logistical problems inherent in securely communicating the secret key to a would-be correspondent (particularly challenging if there are many potential correspondents) and a number of other security-related reasons.[12]

Public key cryptography, in contrast, is well-suited for use on open computer networks.[13] It utilizes two different paired keys: an individual has a "public key," which they make widely available, and a "private key," which is kept secret. One way that public key cryptography can be used is to send confidential messages. If Alice wished to send a message to Bob which only he could read, she would first locate his *public* key, which he may have published in a publicly-accessible online

---

10. *See, e.g.*, SCHNEIER, APPLIED CRYPTOGRAPHY, *supra* note 7, at 31 ("In 1976 Whitfield Diffie and Martin Hellman changed the paradigm of cryptography forever."). Cryptography is the art and science of keeping messages secure; it is practiced by cryptographers. *Id.* at 1. The process of disguising a message in such a way as to hide its substance is called encryption; the process of returning the message to its original form is called decryption. *Id. See also* RSA FAQ, *supra* note 7, at § 1.1 ("Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key.").

11. An algorithm is a mathematical formula that describes the scrambling technique; it does not need to be kept secret. SCHNEIER, APPLIED CRYPTOGRAPHY, *supra* note 7, at 2 - 3.

12. *See* SCHNEIER, E-MAIL SECURITY, *supra* note 7, at 41-42; RSA FAQ, *supra* note 7, at § 1.4.

13. *See* SCHNEIER, E-MAIL SECURITY, *supra* note 7, at 43; RSA FAQ, *supra* note 7, at § 1.4

database. Alice would encrypt the message using his public key (and a public key algorithm) and send it to him. Bob would decrypt the message using his *private* key (and the same public key algorithm). Once the message was encrypted with Bob's public key, only his private key could decrypt the message—so if an eavesdropper intercepted it, they could not read it. Anyone who wanted to send an encrypted message to Bob could go through the same process, even if they had never communicated with Bob before. Public key cryptography eliminates the need for two correspondents to agree upon a secret key.[14]

Computer equipment and software utilizing public key cryptography is sometimes termed an "asymmetric cryptosystem." This term is used in the Utah Act.[15]

B. Digital Signatures

Digital signatures involve reversing the role of public and private key, utilizing public key cryptography to achieve goals other than confidentiality. For example, if Alice encrypted the message to Bob using her *private* key, Bob could decrypt the message using Alice's *public* key, which he might find in a public database. Bob could be assured that

---

14. Public key cryptography utilizes two components, a set of paired keys and an algorithm. A number of different public key cryptographic algorithms exist. These algorithms are proprietary and patentable, and several have been the subject of intense and acrimonious intellectual property disputes. *See The Friendliest of Enemies Shaky Marriage Between Crypto Firms Shatters Cylink, RSA do Battle over Future of Electronic Commerce*, INFO. L. ALERT: A VOORHEES REP., Sept. 9, 1994, *available in* LEXIS, MARKET Library, IACNWS File; *Ugly Till the End Cylink Gains Edge in Crypto Case*, INFO. L. ALERT: A VOORHEES REP., Sept. 29, 1995; *Splitting the Baby, Again RSA-Cylink Arbitrators Revisit Crypto Mess*, INFO. L. ALERT: A VOORHEES REP., Feb. 9, 1996; SCHNEIER, APPLIED CRYPTOGRAPHY, *supra* note 7, at 609-10. Additionally, they can be implemented in different ways. For example, RSA, the leading public key algorithm, can be used for encryption (that is, to provide the quality of confidentiality) as well as to create digital signatures. DSA, a U.S. government endorsed algorithm, can theoretically only be used to create digital signatures—it cannot be used for encryption. Thus, a system which utilized the DSA algorithm alone theoretically could not achieve the quality of confidentiality. *See* SCHNEIER, E-MAIL SECURITY, *supra* note 7, at 45, 47. The use of powerful cryptography by private citizens for the purposes of achieving confidentiality of data messages and files is the source of immense political controversy, pitting law enforcement officials (who want access to all electronic communications) against business interests (who chafe at the current export restrictions on cryptography, *see* International Traffic in Arms Regulations, 22 C.F.R. § 120 (1996)) and civil libertarians. For an excellent summary of the many legal issues implicated in this debate, see A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995). For additional background information, visit the Internet sites of the Electronic Privacy Information Center (EPIC) at <http://www.epic.org> and the Electronic Frontier Foundation (EFF) at <http://www.eff.org>.

15. § 46-3-103(2).

Alice sent the message because if the message can be decrypted using Alice's public key, then it must have been encrypted using her private key. Thus, Alice and Bob have achieved "data origin authentication."

Digital signatures, as contemplated under the Utah Act, involve another step: the one-way hash function. A one-way hash function is a mathematical process that is used to take a message of any length and create a short, fixed-length "hash" unique to that message, called a message digest.[16] Each time a message is run through the hash function it will result in the same value, but no two distinct messages will return the same value.[17] The hash function is "one way" because it is virtually impossible to reconstruct the original message using the message digest.[18]

If Alice wants to "sign" an electronic document with a digital signature and send it to Bob, she does not have to encrypt the entire document with her private key. Instead, she can run the document through a one-way hash function, creating a message digest. She can then encrypt that message digest using her private key and send it along with the unencrypted document. Note that every digital signature is unique to the document for which it is created. So a forger could not take Alice's digital signature from one document, append it to a fraudulent document, and then successfully claim that Alice had signed the fraudulent document.

When Bob receives the message, he independently runs the same one-way hash function on the original message to determine what the message digest should be. He then decrypts (or "verifies") Alice's digital signature, using Alice's public key. If the message digest in Alice's decrypted digital signature matches the message digest that Bob calculated from the message on his own, then Bob knows that the message is indeed from Alice, and that it has not been altered since she signed it. If the message digests are not identical, then Bob knows that Alice did not sign the same message that he received—somehow the message has been altered. If the message digests are identical, Alice cannot later successfully claim that she did not send the message. No

16. RSA FAQ, *supra* note 7, § 8.2.

17. Actually, this is not really true, but "the chances of any two messages hashing to the same value are minute enough to be negligible." SCHNEIER, E-MAIL SECURITY, *supra* note 7, at 60.

18. *Id.* at 59. ("[T]here is no way to go backwards with a one-way hash function.")

one else could have created the digital signature attached to the document. Thus Alice and Bob may have achieved the qualities of data origin authentication, message integrity, and non-repudiation.[19]

C. *Certificates and Certification Authorities*

Although the procedure followed by Alice and Bob offers the possibility of achieving data origin authentication, message integrity, and non-repudiation, they did not *actually* achieve all of these qualities because of a fundamental problem in asymmetric cryptosystems: identification of the sender. Alice may not have sent the message to Bob at all. Instead, a forger may have generated a key pair and entered the public key in a public key database under the name "Alice." Bob may enter into a business arrangement whereby Bob performs some service for the person he believes to be Alice. When Bob later attempts to enforce his electronic contract and collect from the real Alice, he will find that he has been the victim of fraud. Certificates attempt to solve this problem of identification.

Certificates are digitally-signed electronic documents that attest to the connection of a public key to an individual (or other entity).[20] Certificates are issued by certification authorities (CAs). The process might work like this. Alice would generate her public and private key pair.[21] She would then take her public key (on a floppy disk, for example) to a CA and present some form of identification. The CA would check the identification and take any other steps necessary to assure itself that Alice was indeed who she claimed to be. The CA would then give

---

19. Note that Alice and Bob have not achieved confidentiality, a critical security service. While digital signatures utilize public key cryptography, they do not, by themselves, provide this quality of confidentiality. Alice can send Bob an unencrypted (or "plaintext") message with a digital signature attached. This digital signature can prove that the message in fact came from Alice and that the message has not been altered. However, someone who intercepted the message could read it, and verify the digital signature.

20. RSA FAQ, *supra* note 7, § 3.5.

21. Generating key pairs is not a simple process. One part of the process involves generating random numbers. Bruce Schneier notes: "If there is a flaw in the algorithm that generates the random numbers, then that flaw might be exploitable by an adversary to break the system. This is a tough problem . . . . Imagine what would happen if the program didn't do random-number generation correctly. The program might only generate 10 million public-key/private-key pairs. This would be large enough so that no two users would have the same key, but small enough for a computer to search them all. Even though the program used RSA and DES [two powerful cryptographic algorithms], breaking the system would be easy." SCHNEIER, E-MAIL SECURITY, *supra* note 7, at 51. Indeed, this problem occurred recently in Netscape's implementation of the RSA algorithm in their Navigator World Wide Web browsing software. *See* Steven Levy, *Wisecrackers*, WIRED, Mar. 1996, at 128, 200.

Alice a certificate attesting to the connection between Alice and her public key. The certificate would contain Alice's name, her public key, and some other information. The certificate would be signed using the digital signature of the CA. Thus the certificate could not be altered or forged.

The CA must also somehow prove that it is bound to its public key, which is used to verify Alice's certificate. Thus, the CA would have its own certificate, signed with the digital signature of a "higher level" certification authority. This higher level certification authority might be (as under the Utah Act) a government agency.[22]

Alice would probably choose to publish this certificate in a publicly-accessible online database, so that anyone she corresponded with could verify her digital signature. Thus, when Bob received a message from Alice signed with Alice's digital signature, he could locate Alice's certificate in this online database. If the signature on the message could be verified using the public key listed in the certificate (and if the CA's signature were verified as well), Bob would know that a CA had authenticated Alice's identity, and that he was not dealing with someone else posing as Alice.

D. Certificate Revocation

Certificates are used to address the problem of identification. Public key cryptography presents another vexing problem, however: the security of private keys. If a forger somehow discovers Alice's private key, that forger can digitally sign Alice's name on documents. If a forger discovered a certification authority's private key, that forger would

22. The hierarchy of certification authorities envisioned in the Utah Act is rather "flat" compared to other proposed implementations of a public key infrastructure. Privacy Enhanced Mail (PEM), a draft Internet standard developed by the Privacy and Security Research Group of the Internet Activities Board, envisions a certification hierarchy with at least one additional tier. Under PEM, the Internet PCA Registration Authority (IPRA) serves as the top-level certification authority (the role played by the Division under the Utah Act). The IPRA certifies Policy Certification Authorities (PCAs), who in turn certify certification authorities (CAs) who meet each PCAs particular requirements (different PCAs will have different certification guidelines, i.e., some may be "high-assurance," others may be "mid-level assurance," etc.). For a general overview of the PEM certification framework, see SCHNEIER, E-MAIL SECURITY, *supra* note 7, at 125-27. A more detailed summary of PEM is found in Steven T. Kent, *Internet Privacy Enhanced Mail*, 36:8 COMMUNICATIONS OF THE ACM 48 (1993).

have the means to commit widespread fraud.[23] As a practical matter, in any large-scale system utilizing public key cryptography some private keys will become compromised, and the certificate containing the corresponding public key will need to be revoked. Certificates may have to be revoked for other reasons as well.[24] Certificate revocation lists (CRLs) prevent people from relying on a compromised or otherwise revoked public key/private key pair.

A CRL is a list of public keys that have been revoked prior to their expiration date.[25] If the private key is compromised, or the key pair is no longer in use for some other reason, the public key would be placed on a CRL. Thus, before Bob relied on the electronic message that he received from Alice, he would check to make sure that Alice's certificate was not on a CRL. The online database which published public keys would most likely also maintain a CRL.[26]

---

23. *See* RSA FAQ, *supra* note 7, § 3.10 ("A compromised CA key is a . . . dangerous situation. An attacker who discovers a certifying authority's private key can issue phony certificates in the name of the certifying authority, which would enable undetectable forgeries; for this reason, all precautions must be taken to prevent compromise . . . .").

24. For example, a person may be issued a certificate which enables them to digitally sign documents on behalf of their employer in the course of their employment. If that person leaves their job, their certificate may need to be revoked.

25. Certificates would generally have expiration dates to ensure that the underlying algorithms could not be "broken" by a long term "attack." *See* RSA FAQ, *supra* note 7, § 3.12.

26. This Comment does not explore the issue further, but note the privacy implications of CRLs. The online database that maintains a CRL will have access to valuable transaction-generated information that could expose sensitive relationships among individuals or businesses. If Company A sends a digitally signed message to Company B, Company B must verify the digital signature by connecting to a database, verifying the digital signature and making sure that Company A's certificate is not on a certificate revocation list. This process, of course, will leave electronic footprints. Could the manager of the database disclose the fact that A and B were corresponding? What if A and B were discussing a possible merger or other transaction with significant consequences in the securities markets? Similarly, could the database disclose to Joe Whistleblower's defense-contractor employer that Whistleblower was verifying digital signatures of a reporter from the New York Times? Could the database manager take note of the fact that subscriber C frequently corresponded with a cardiologist's office, and sell C's name, address, or other personal information to a drug company interested in marketing a new drug for heart patients? The Utah Digital Signature Act is totally silent on this and other privacy issues. Lawmakers contemplating digital signature legislation could look to the Customer Proprietary Network Information (CPNI) provisions of the Telecommunications Act of 1996 for guidance on how customer privacy is protected in an analogous context. *See* Telecommunication Act of 1996, 104 Pub. L. No. 104, § 702, 110 Stat. 56 (1996) (creating 47 U.S.C. § 221). *See also, e.g.*, CAL. PUB. UTIL. CODE § 2891 (West Supp. 1996).

III. THE UTAH DIGITAL SIGNATURE ACT

The Utah Digital Signature Act provides a regulatory scheme for licensing CAs and certificate databases (termed "recognized repositories"), allocates liability and evidentiary burdens among participants in the public key infrastructure implemented by the Act, and addresses the legal status of electronic documents signed with digital signatures created using licensed CAs. The Act is divided into five parts. A part-by-part general overview of the Act follows.[27]

Part I of the Utah Act sets out the purposes of the Act, general interpretive instructions, a long list of definitions, and guidelines concerning the role of the Utah Department of Commerce Division of Corporations and Corporate Code ("Division") in implementing the Act. The Act states that its goal is to effectuate the following purposes:

(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, such as X.509 of the International Telecommunication Union[28] . . .; and
(4) to establish, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages.[29]

After stating the Act's purposes, Part I moves to a comprehensive list of definitions. The definitions in the Utah Act largely mirror the definitions presented in the Information Security Committee's Digital Signature Guidelines,[30] and generally promise to be a useful model for other legislative efforts, even those that differ from the Utah Act.

---

27. Some differences between the amended 1996 version of the Act and the 1995 original version are noted. At least one state that is contemplating digital signature legislation has modeled its proposed statute after the original 1995 version of the Utah Act. *See* 1995 Haw. Sess. Laws 203.

28. X.509 is a standard format for certificates. It was developed by the International Telecommunications Union (then known as the International Consultative Committee on Telephony and Telegraphy and abbreviated as "CCITT") in 1988, and amendments were proposed in late 1995. *See* RSA FAQ, *supra* note 7, § 3.5.

29. § 46-3-102.

30. See *infra* note 118 and accompanying text.

Part I also describes the role of the Division, an entity similar to the Secretary of State's office in many other states.[31] The commentary to the relevant provision of the Act describes the Division's role as follows:

> As a certification authority, the Division's role should be limited, in the main, to (1) spawning other certification authorities, who . . . do most of the work of issuing certificates to the private sector, (2) enabling licensed certification authorities within state government to act as certification authorities, and (3) serving users within the Division itself . . . . For the private sector, the Division could essentially be a "prime mover" in issuing certificates, issuing only as many certificates as needed to start the mainly private-sector digital signature infrastructure functioning . . . .
>
> The principal role of the Division lies, not in acting as a certification authority in its own right, but rather in policy making, facilitating implementation of digital signature technology as needed, and regulatory oversight.[32]

In addition to serving as a top-level certification authority, the Division has broad rulemaking authority.[33] Among other things, the Division is authorized to assure the financial responsibility of CAs by "determin[ing] an amount appropriate for a suitable guaranty, in light of: (i) the burden a suitable guaranty places upon licensed certification authorities; and (ii) the assurance of financial responsibility it provides to persons who rely on certificates issued by licensed certification authorities."[34] A suitable guaranty is either a surety bond or an irrevocable letter of credit that meets certain administrative specifications[35] and is designed to facilitate collection of any judgment obtained against a CA. The Act states that "[a] suitable guaranty may also provide that the total annual liability on the guaranty to all persons making claims based on it may not exceed the face amount of the guaranty."[36] Financial institutions acting as certification authorities are exempted from the requirement of posting a suitable guaranty.[37]

In addition to addressing the suitable guaranty issue in rulemaking proceedings, the Division is authorized to "review software for use in creating digital signatures and publish reports concerning software."[38] The Division is also authorized to make rules concerning the form of

---

31. UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 34.
32. *Id.* at 36.
33. § 46-3-104(3).
34. § 46-3-104(3)(b).
35. § 46-3-103(33)(a).
36. § 46-3-103(33)(b).
37. § 46-3-103(33)(c).
38. § 46-3-104(3)(c). The 1995 version of the Act empowered the Division to "approve asymmetric cryptosystems for use in signing certificates issued by licensed certification authorities," and to issue rules addressing the "suitability of algorithms for use in fulfilling the requirements of this chapter." 1995 Utah Laws 46-3-501(4), 46-3-501(5)(c).

certificates, record-keeping requirements for certification authorities, and the form and content of certification authority disclosure records (publicly-accessible documents which detail certain specified practices of certification authorities), and to promulgate other rules necessary to effectuate the Act.[39]

Part II of the Act turns to the licensing and regulation of certification authorities. The Act sets out minimum qualifications that a certification authority must meet in order to obtain a license. Licensing is voluntary; unlicensed CAs can operate in the state. Among a number of other requirements (such as providing a suitable guaranty, "employ[ing] as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of this chapter," and being the subscriber of a certificate published in a recognized repository), licensed certification authorities must "have the right to use a trustworthy system, including a secure means for controlling usage of its private key."[40] "Trustworthy system" is defined as computer hardware and software which (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; and (c) are reasonably suited to performing their intended functions.[41] The 1995 Utah Act limited the availability of certification authority licenses to Utah-licensed attorneys, financial institutions, title and escrow companies, and certain public entities.[42] The 1996 amendments dropped these restrictions.

The Division is empowered to issue restricted licenses under certain circumstances.[43] The Division may also revoke or suspend a CA's

39. § 46-3-104(3).
40. § 46-3-201(1).
41. § 46-3-103(37).
42. UTAH CODE ANN. § 46-3-201 (Supp. 1995) (repealed 1996). *See also* Memorandum from Alan Asay to the Digital Signature Legislative Facilitation Committee, Aug. 26, 1994 (recommending that licensed CAs be limited to Utah State Bar members in good standing or their law firms, financial institutions, insurance companies, and title companies, because of the prospect of unscrupulous behavior by a CA) (copy on file with author).
43. The Division may issue restricted licenses classified according to specified limitations such as a maximum number of outstanding certificates, cumulative maximum of recommended reliance limits in certificates issued by the certification authority, or issuance only within a certain firm or organization. § 46-3-201(3).

license for failure to comply with the requirements of the Act, including failure to maintain the minimum qualifications specified in the Act.[44]

The Division may, by administrative rule, recognize CAs licensed or authorized by other governmental entities, "provided that those licensing or authorization requirements are substantially similar to those of this state."[45] If the Division recognizes the licensing of a CA by another governmental entity, Part IV of the Utah Act (which establishes certain presumptions for adjudicating disputes involving digital signatures and details the legal effects of digital signatures created through the use of licensed CAs) and certain liability limitations granted to licensed CAs in Part III of the Act both apply in the same fashion to the out-of-state licensed CA as they apply to Utah-licensed certification authorities.[46] These provisions explicitly *do not* apply to digital signatures created using unlicensed CAs.[47]

Performance audits are also described in Part II of the Utah Act. Licensed CAs are required to have annual performance audits of their operations, performed by a certified public accountant having expertise in computer security or an accredited computer security professional (additional qualifications for auditors may be specified by Division rule).[48] Exemptions are allowed under certain circumstances.[49]

Part II lastly describes the enforcement powers of the Division. The Division can investigate the activities of licensed CAs and issue orders designed to further its investigation and secure compliance with the requirements of the Act.[50] Civil penalties can be assessed for violations of the Act committed knowingly or intentionally, up to $5,000 per violation or 90% of the "recommended reliance limit" of a material

---

44. § 46-3-201(4). This section requires that revocation or suspension of licensure must take place in accordance with the procedures for adjudicative proceedings prescribed by Utah's Administrative Procedures Act, codified at UTAH CODE ANN. §§ 63-46b-0.5 to -22 (1993).

45. § 46-3-201(5).

46. *Id.*

47. § 46-3-201(6). Concerning unlicensed certification authorities, the commentary to this portion of the Act notes:

> [A] digital signature may be effective, enforceable, and valid even though it is verified only by a certificate issued by an unlicensed certification authority. This Act does not preclude the application of other laws for determining what constitutes a signature; a mark such as a digital signature may be a valid signature under law other than this Act . . . . A certification authority who chooses to operate in this state without a license would undertake greater risk of liability . . . .

UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 39.

48. § 46-3-202(1).

49. § 46-3-202(3).

50. § 46-3-203(1).

certificate, whichever is less.[51] The Division is also empowered to "issue orders and obtain injunctions or other civil relief" against any certification authority, licensed *or unlicensed*, which is conducting its business in such a manner as to create an unreasonable risk of loss to subscribers of that certification authority, or to a repository.[52]

Part III of the Utah Digital Signature Act turns to the duties of certification authorities and subscribers (persons utilizing the services of a CA). CAs are required to use trustworthy systems,[53] and are required to disclose the practices they employ in issuing certificates, upon specific request and payment of reasonable compensation.[54]

Prior to issuing a certificate to a subscriber, a certification authority must satisfy several conditions. Along with several other technical requirements, the Act requires that the CA must confirm that:

(i) the prospective subscriber is the person to be listed in the certificate to be issued;
(ii) if the prospective subscriber is acting through one or more agents, the subscriber authorized the agent or agents to have custody of the subscriber's private key;
(iii) the information in the certificate to be issued is accurate; and
(iv) the prospective subscriber rightfully holds the private key[55]

---

51. § 46-3-203(3). "Recommended reliance limit" is a monetary amount. § 46-3-103(28). By specifying a recommended reliance limit is a certificate, the issuing CA and the accepting subscriber recommend that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit. § 46-3-309(1).

52. § 46-3-204(1) and (3). This Comment does not explore the issue further, but the grant of authority to act against unlicensed certification authorities is rather remarkable. As discussed very briefly in note 14, *supra*, encryption technology has sparked very heated political controversy. One phenomenon that fueled this controversy was the release and subsequent widespread adoption of a powerful encryption program, "Pretty Good Privacy" (PGP), on the Internet. PGP users act as certification authorities for other PGP users, establishing a non-hierarchical "web of trust" certification scheme that is very different from the certification hierarchy implemented by the Utah Act. *See generally* SIMSON L. GARFINKEL, PGP: PRETTY GOOD PRIVACY (1995). Use of powerful encryption like PGP is generally disfavored by law enforcement officials. Would these provisions of the Utah Act allow a zealous official to take legal action against a particular PGP user/"certification authority" under the ostensible rationale that PGP's "web of trust" certification scheme inherently creates unreasonable risk?

53. § 46-3-301(1).

54. § 46-3-301(2).

55. "'Rightfully hold a private key' means to be able to utilize a private key: (a) which the holder or the holder's agents have not disclosed to any person . . .; and (b) which the holder has not obtained through theft, deceit, eavesdropping, or other unlawful

corresponding to the public key to be listed in the certificate.[56]

These requirements cannot be waived or disclaimed by either the CA or a subscriber.[57]

By issuing a certificate, a CA makes certain warranties to the subscriber named in the certificate. These include warranting that the certificate contains no information known to the CA to be false, and warranting that the certificate "satisfies all material requirements" imposed by the Act.[58] The CA cannot disclaim or limit these warranties.[59] The Act also imposes ongoing obligations to the subscriber on the CA, which can be altered by contrary agreement. The CA is obligated to promptly suspend or revoke a certificate when specified conditions are satisfied, and is obligated to notify the subscriber of any facts which significantly affect the validity or reliability of the subscriber's certificate after it is issued.[60] By issuing a certificate, a CA certifies to all who reasonably rely on it that, among other things, the information in the certificate is accurate and that the subscriber has accepted the certificate.[61]

Accepting a certificate imposes duties on a subscriber. By accepting a certificate issued by a licensed CA, a subscriber certifies to all who reasonably rely on the certificate that the subscriber rightfully holds the private key corresponding to the public key listed in the certificate, and that all representations made by the subscriber to the CA or otherwise incorporated into the certificate are true.[62] Agents or purported agents who accept a certificate on behalf of a principal personally certify that they have legal authority to act on behalf of the principal, and that adequate safeguards exist to prevent the agent from exceeding the bounds of any limitations on that agent's ability to sign digitally on behalf of the principal.[63] Accepting a certificate imposes indemnification obligations on a subscriber:

> By accepting a certificate, a subscriber undertakes to indemnify the issuing certification authority for any loss or damage caused by issuance or publication of a certificate in reliance on:
> (a) a false and material representation of fact by the subscriber; or
> (b) the failure of the subscriber to disclose a material fact;

---

means." § 46-3-103(31).
56. § 46-3-302(1)(b).
57. § 46-3-302(1)(c).
58. § 46-3-303(1)(a) and (b).
59. § 46-3-303(1).
60. § 46-3-303(2).
61. § 46-3-303(4).
62. § 46-3-304(1).
63. § 46-3-304(2).

> if the representation or failure to disclose was made either with intent to deceive the certification authority or a person relying on a certificate, or with negligence. . . . The indemnity provided in this subsection may not be disclaimed or contractually limited in scope . . . .[64]

By accepting a certificate, a subscriber assumes a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in the certificate, and to prevent its disclosure to any person not authorized to create the subscriber's digital signature.[65] A private key is deemed to be the personal property of the subscriber who rightfully holds it.[66] A CA who holds a subscriber's private key does so as a fiduciary, and may use the private key only with the subscriber's express permission.[67]

CAs are required to publish certificates which they have issued in a recognized repository[68] unless a contract between a subscriber and the CA provides otherwise.[69] After issuing a certificate, a CA can suspend or revoke it under certain conditions, including upon the subscriber's request.[70] Likewise, the Division can order a CA to revoke or suspend a certificate if certain conditions are met, including compliance with the Administrative Procedures Act by the Division.[71] Notice of suspension or revocation must be "immediately" published in a recognized repository specified in the certificate.[72] While a particular certificate is suspended, a subscriber is released from the duty to keep the relevant private key secure.[73] Upon notice of revocation, a subscriber is

---

64. § 46-3-304(4).
65. § 46-3-305(1). The commentary to this portion of the Utah Act offers three alternative standards of care for holders of private keys: strict liability, diligence, and "negligence for consumers; diligence for others." UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 50. Some of the drafters of the Utah Act originally advocated a strict liability standard for breach of the duty to safeguard a subscriber's private key. *See* Memorandum from Alan Asay to the Digital Signature Legislative Facilitation Committee, Aug. 24, 1994 (recommending strict liability standard) (copy on file with author).
66. § 46-3-305(2).
67. § 46-3-305(3).
68. Repositories are on-line databases of certificates available for retrieval and use in verifying digital signatures. UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 13. Recognized repositories are repositories recognized by the Division pursuant to § 46-3-501. § 46-3-103(27).
69. § 46-3-302(2).
70. §§ 46-3-302(4), -306, -307.
71. § 46-3-302(5).
72. §§ 46-3-306(3), -307(5).
73. § 46-3-306(7).

released from the duty to keep the private key secure and from the other duties imposed by the acceptance of a certificate.[74] Revocation also releases a CA from its warranties and representations.[75] These duties are also discharged upon the expiration of a certificate; all certificates are required to have an expiration date.[76]

Liability limits for licensed CAs are detailed. The Act provides that, unless waived by the CA, a CA shall:

> (a) not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with all material requirements of [the Act];
> (b) not be liable in excess of the amount specified in the certificate as its recommended reliance limit for either:
> (i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or
> (ii) failure to comply with section 302[77] in issuing the certificate;
> (c) be liable only for direct, compensatory damages in any action to recover a loss due to reliance on the certificate. Direct compensatory damages do not include:
> (i) punitive or exemplary damages;
> (ii) damages for lost profits, savings, or opportunity; or
> (iii) damages for pain and suffering.[78]

Part III lastly provides rules for collection upon a suitable guaranty. A claimant may recover the full amount of a "qualified right to payment" against the surety bond or letter of credit serving as the suitable guaranty.[79] A qualified right to payment means an award of damages against a licensed CA by a court having jurisdiction over the CA in a civil action for violation of the Act.[80] In addition to the amount of the qualified right to payment, a claimant can recover reasonable attorney's fees and court costs from the suitable guaranty.[81] The total liability on the suitable guaranty to all persons making qualified rights of payment or recovering attorney's fees during its term cannot exceed the amount of the suitable guaranty.[82] Interpleader techniques will assist in equitably distributing the proceeds of a suitable

---

74. § 46-3-307(6).
75. § 46-3-307(7).
76. § 46-3-308(1) to (2).
77. § 46-3-302 details the requirements that must be met prior to a CA issuing a certificate to a subscriber.
78. § 46-3-309(2).
79. § 46-3-310(1).
80. § 46-3-103(25).
81. § 46-3-310(2).
82. § 46-3-310(1) to 46-3-310(2).

guaranty to multiple claimants whose claims exceed the amount of the guaranty.[83]

Part IV of the Act addresses the effect of a digital signature. A digital signature is deemed to satisfy legal signature requirements if:

> (1) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;
> (2) that digital signature was affixed by the signer with the intention of signing the message; and
> (3) the recipient has no knowledge or notice that the signer either:
> (a) breached a duty as a subscriber; or
> (b) does not rightfully hold the private key used to affix the digital signature.[84]

Language in the Act and in the accompanying commentary emphasizes that the Act is not designed to preclude other symbols or marks from being valid as a signature under other applicable law. "An unverified digital signature or other symbol may be treated as a signature, if, in the words of the Uniform Commercial Code § 1-201(39), it is 'executed or adopted by a party with the present intention to authenticate a writing.'"[85] The Act is designed to "appl[y] only to the digital signatures described within it, and . . . simply does not pertain to the validity of other symbols as signatures."[86]

If reliance on a digital signature is "not reasonable under the circumstances," the recipient of that digital signature assumes the risk that digital signature is forged.[87] A recipient of a digital signature can determine not to rely on an unreliable signature and must promptly notify the signer of that decision.[88]

The Act states that electronic documents signed with a valid digital signature created using a licensed CA are "written" as required by the statute of frauds.[89] Additionally, a copy of a digitally signed message is "as effective, valid, and enforceable as the original of the message," thus satisfying the best evidence rule.[90]

---

83. UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 60.
84. § 46-3-401.
85. UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 61.
86. *Id.*
87. § 46-3-402.
88. § 46-3-402.
89. § 46-3-403; UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 64.
90. § 46-3-404. This section contains an exception for originals intended to be unique, such as negotiable instruments. *See* UTAH DIGITAL SIGNATURE LAW, *supra* note

The Act provides that a certificate issued by a licensed CA is an acknowledgment of a digital signature verified by reference to the public key listed in the certificate.[91] Thus, among other things, digitally signed documents are deemed to be "acknowledged" and self-authenticating and are therefore *prima facie* admissible evidence under rule 902(8) of the Utah Rules of Evidence (identical to rule 902(8) of the Federal Rules of Evidence).[92]

Presumptions for adjudicating disputes are set out in the Act as follows:

> In adjudicating a dispute involving a digital signature, a court of this state shall presume that:
> (1) A certificate digitally signed by a licensed certification authority and either published in a recognized repository or made available by the issuing certification authority or by the subscriber listed in the certificate is issued by the certification authority which digitally signed it and is accepted by the subscriber listed in it;
> (2) The information listed in a valid certificate . . . and confirmed by a licensed certification authority issuing the certificate is accurate;
> (3) If a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority:
> (a) that digital signature is the digital signature of the subscriber listed in that certificate;
> (b) that digital signature was affixed by the signer[93] with the intention of signing the message; and
> (c) the recipient of that digital signature has no knowledge or notice that the signer:
> (i) breached a duty as a subscriber; or
> (ii) does not rightfully hold the private key used to affix the digital signature; and
> (4) A digital signature was created before it was timestamped by a disinterested person utilizing a trustworthy system.[94]

The commentary to this section of the Act claims that "[t]he effect of the presumptions provided in this section is merely to allocate the burden of

---

1, at 65.

91. § 46-3-405.

92. UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 66-67.

93. As drafted by Utah Digital Signature Legislative Facilitation Committee the 1996 amendments to the Utah Act used the words "that subscriber" rather than "the signer." *See* UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 68. Presumably the Utah legislature did not intend to substantively alter the meaning of this section by this eleventh-hour change (an assumption that is buttressed by reading subsection 3(b) in conjunction with subsection 3(a)). Rather, the legislature probably made the change in order to echo the language in § 46-3-401, which establishes the legal status of digital signatures. At least one other state that has followed the Utah Act model has retained the original language, "that subscriber." *See* S. 6423, 54th Leg., Reg. Sess. § 406 (Wash. 1995).

94. § 46-3-406.

going forward with allegations and evidence to the party challenging the digital signature, the certificate, or the trustworthy time-stamp."[95]

Part V of the Act concerns repositories. The Division is required to recognize one or more repositories.[96] A recognized repository must be operated by a licensed CA and provide access to a database containing certificates published by the repository, notices of suspended or revoked certificates, certification authority disclosure records for licensed CAs, and other information specified by the Division.[97] Procedures for recognition of repositories are set out in the Act[98] and in accompanying regulations.[99]

The liability of recognized repositories is limited by the Act. Unless waived, a recognized repository, or the owner or operator of a recognized repository, is not liable for failure to record suspension or revocation of a certificate unless more than one business day elapsed after notice was received.[100] However, the repository may be held liable for any loss of a person who relied on a revoked or suspended certificate—up to the amount of the recommended reliance limit on the relevant certificate and including only direct compensatory damages and not punitive damages or lost profits, savings, or opportunity—if the repository failed to publish notice of suspension or revocation of a certificate more than one business day after receiving notice.[101] Repositories are not liable for misrepresentation in a certificate published by a licensed certification authority.[102] Nor are they liable for publishing information which the Division requires them to publish.[103]

---

95. UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 69. As discussed in Section V of this Comment, however, the Act may impose a greater evidentiary burden than suggested in the commentary. A time-stamp is a digitally-signed notation appended or attached to a message which indicates, at least, the date and time when the notation was created and the identity of the person creating the notation. § 46-3-103(36). Reliable time-stamps are essential to maintain the validity of electronic documents over many years. RSA FAQ, *supra* note 7, § 3.18.

96. § 46-3-501(2).

97. §§ 46-3-501(2)(a) to -501(2)(b).

98. § 46-3-501(2).

99. UTAH ADMIN. R. 146-10-401 (1996).

100. § 46-3-502(2)(a).

101. § 46-3-502(1) - (2).

102. § 46-3-502(2)(a)(iii)).

103. § 46-3-502(2)(a)(v).

IV. THE UTAH DIGITAL SIGNATURE ACT AS PUTATIVE "MODEL ACT"

The Utah Digital Signature Act was developed in collaboration with the Information Security Committee of the Section of Science and Technology of the American Bar Association (the "Information Security Committee").[104] The Information Security Committee, which endorsed the Utah Act "in principle,"[105] planned to release a Model Digital Signature Act in June of 1995.[106] The release of this draft model legislation has been delayed indefinitely. One report credits "bureaucratic maneuvering" for the delay, describing the frustration of Information Security Committee members over the postponement of the release of their Model Act.[107] The Information Security Committee had been developing model legislation for three years. Committee member's frustration reportedly was compounded by the specter of rapidly accelerating state legislative activity concerning digital signatures, proceeding without the guidance of the Information Security Committee's model legislation.[108]

In the absence of model legislation from the Information Security Committee, a number of states turned to the Utah Act as model digital signature legislation, a process encouraged by the drafters of the Utah legislation.[109] In several public communications, a prominent Informa-

---

104. UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 18.

105. Resolution of the Information Security Committee, Section of Science and Technology, American Bar Association (November 9, 1994) (copy on file with author).

106. E-mail message from Michael S. Baum, Chair of the Information Security Committee, Section of Science and Technology, American Bar Association, to the <ca-digsig@commerce.net> Internet mailing list (May 6, 1995) (printed copy on file with author).

107. *Digital Signature Maven Bye Bye Baum ABA EDI and Information Technology Division Head Resigns*, INFO. L. ALERT: A VOORHEES REP., Oct. 13, 1995, *available in* LEXIS, MARKET Library, IACNWS File ("the ABA's work at providing states with a draft bill has been stymied by bureaucratic maneuvering").

108. *ABA Model Law on Digital Signature on Hold*, INFO. L. ALERT: A VOORHEES REP., Sept. 8, 1995, *available in* LEXIS, MARKET Library, IACNWS File ("The delay has angered some members of the Information Security Committee who fear that state legislative action is moving too fast for the ABA to have much influence.");

109. *See, e.g.*, § 46-3-102(4) (one of the purposes of the Utah Act is to establish, in coordination with other states, uniform rules for digital signatures). *See also* UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 25 (noting that one of the purposes for publishing the commentary is to provide guidance for other states considering digital signature legislation). The Utah Department of Commerce, Division of Corporations and Commercial Code formed an "interjurisdictional group" which held at least one "discussion meeting." Among the suggested topics at this meeting was "What should we do to facilitate this new approach to commerce?" Proposed Agenda for Discussion Meeting on Interstate Cooperation Regarding Digital Signatures (undated) (copy on file

tion Security Committee member who was also involved in the drafting of the Utah Act indicated that the "U.S. Model Digital Signature Act" under development by the Information Security Committee was substantively identical to the Utah Digital Signature Act.[110] At its September 19, 1995 meeting, the Utah's Digital Signature Legislative Facilitation Committee, the *ad hoc* committee which drafted the Utah Act, discussed the delay in the release of the Information Security Committee's Model Act. The minutes of the meeting note that, "despite efforts by the ABA or NCCUSL,[111] the perception held by many states is that Utah's Act is the Model Act. Therefore, it was determined that Utah's interest, and the interests of other jurisdictions, require amending the Utah Act in conformity with the work of the ABA Committee."[112]

The explanation for the delay of the Information Security Committee's model legislation appears to be more complex than simply "bureaucratic maneuvering," and the picture painted by the proponents of the Utah Act as a model act may be misleading. One Committee member has indicated that the primary reason for the lack of a legislative recommendation from the Information Security Committee was that a "majority" of the committee believed "digital signature legislation like Utah's is

---

with author); Letter from George Danielson, Digital Signature Coordinator, Utah Department of Commerce, to C. Bradford Biddle (February 14, 1996) (describing this group as the "interjurisdictional group") (on file with author). *See also* § 46-3-201(5) (providing that the Utah Department of Commerce Division of Corporations and Commercial Code can recognize certification authorities licensed or authorized by another state if the licensing or authorization requirements of the other state are "substantially similar" to those of Utah).

110. Alan Asay was the principal drafter of the Utah Act and also served as a Reporter for the Information Security Committee's effort. In an e-mail message to Barry Fraser of the Privacy Rights Clearinghouse, Asay wrote: "The Act adopted in Utah and under consideration in other states is about to be published, with some revision and for comment, as the Model Digital Signature Act by the American Bar Association's Information Security Committee." E-mail message from Alan Asay (April 29, 1995) (printed copy on file with author). In an e-mail message to the "ca-digsig" mailing list, Asay wrote that he expected the proposed amendments to the Utah Act (since enacted) to "largely if not entirely conform the Act as it now stands to the ABA ISC's US Model Digital Signature Act." E-mail message from Alan Asay to the <ca-digsig@commerce.net> mailing list (May 6, 1995) (printed copy on file with author.)

111. National Conference of Commissioners on Uniform State Laws. See *infra* note 114.

112. Minutes of the Utah Digital Signatures [*sic*] Act, Legislation Facilitation Committee (September 19, 1995) (on file with author).

simply unnecessary."[113] Michael Baum, Chair of the Information Security Committee, has noted that the committee's decision not to proceed with model legislation was the result of a number of legitimate factors, including "a probable lack of consensus [among committee members] on a single legislative approach . . . ."[114]

In spite of some resistance to the Utah approach within the Information Security Committee and elsewhere, a number of states are moving forward with digital signature legislation modeled upon the Utah Act. By April of 1996, at least nine states had passed or had actively considered digital signature legislation.[115] Five of these states (Arizona, Georgia, Hawaii, Michigan, and Washington) were considering or had enacted bills directly modeled after the Utah Act.[116] California enacted a different, narrower form of digital signature legislation in 1995, and a bill modeled after this legislation was introduced in Rhode Island in 1996. Legislation in Florida[117] and Virginia focused primarily on studying the issue of digital signature legislation and reporting findings to the legislature.

On October 5, 1995, the Information Security Committee released an exposure draft of its Digital Signature Guidelines, which it described as "general, abstract statements of principle, intended to serve as long-term,

---

113. E-mail message from Peter N. Weiss, Information Security Committee member, to C. Bradford Biddle (February 23, 1996) (printed copy on file with author).

114. E-mail message from Michael Baum to the <ca-digsig@commerce.net> mailing list (February 21, 1996) (printed copy on file with author). Baum's message noted that

> our decision not to proceed with model legislation was the result of many legitimate factors, including (1) notice from the National Conference of Commissioners on Uniform State Laws to our section that they are considering the possibility of drafting model legislation (and the ABA's agreement with the Commissioners to coordinate such matters), (2) the fact that our committee has not yet had the time to rigorously consider and debate legislative issues and approaches . . ., (3) our committee's legitimate focus on the completion of the draft Digital Signature Guidelines (the current focus of considerable effort), and (4) a probable lack of consensus on a single legislative approach at this time.

115. *See* H.R. 2444, 42nd Leg., 2d Reg. Sess. (Ariz. 1996); A. 1577, ch. 594 (Cal. 1995); H.R. 1023 (Fla. 1996); S. 942 (Fla. 1996); S. 736, Reg. Sess. (Ga. 1995); H.R. 1256, Reg. Sess. (Ga. 1995); S.R. 621, Reg. Sess. (Ga. 1995); S. 2401, 18th Leg. (Haw. 1995); S. 939, 1996 Sess. (Mich. 1995); G.A. 8125, Jan. Sess. (R.I. 1995); H.R.J. Res. 195 (Va. 1996); S. 5959, 54th Leg., Reg. Sess. (Wash. 1995); S. 6423, 54th Leg., Reg. Sess. (Wash. 1995).

116. Washington enacted 1995 Senate Bill 6423 on March 29, 1996. 1995 Washington Senate Bill 5959 died. The Oregon legislation died in committee in 1995. 1996 Arizona House Bill 2444 was enacted on April 18, 1996, but amendments caused it to no longer follow the Utah model. 1995 Georgia Senate Bill 736 died in committee on March 8, 1996. 1995 Hawaii Senate Bill 2401 was enacted on June 17, 1996. The other legislation was pending as of this writing.

117. Florida enacted digital signature legislation that differs both from the Utah model and from California's approach on May 25, 1996. S. 942 (Fla. 1996).

unifying foundations for digital signature law across varying legal settings."[118] The Guidelines, while comprehensive, are not intended to serve as model legislation, and they avoid taking positions on many critical issues that legislation in this area must address.[119]

V. CRITICISM OF THE UTAH ACT

The remainder of this Comment focuses on one problem area for the Utah Digital Signature Act: the allocation of liability and evidentiary burdens.[120] Under the Utah Digital Signature Act, users of digital

---

118. INFORMATION SECURITY COMMITTEE, AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES 20 (Draft, October 5, 1995) [Hereinafter DRAFT DIGITAL SIGNATURE GUIDELINES]. On August 1, 1996 the Information Security Committee released the final version of these guidelines. INFORMATION SECURITY COMMITTEE, AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE (1996).

119. *See, e.g.*, DRAFT DIGITAL SIGNATURE GUIDELINES, *supra* note 118, § 4.3.2 (noting that the Guidelines are "intentionally silent" on the duty of care required of holders of private keys).

120. There are many other aspects of the Utah Act that deserve critical analysis but will not be discussed here. A thoughtful criticism of public key cryptography generally can be found in WRIGHT, *supra* note 3, § ET1.2. The provisions of the Act relating to the legal status of electronic documents have been criticized as unnecessary and potentially dangerous, in that they arguably unsettle what is already a fairly well-settled body of law. *See generally* Peter N. Weiss, *Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Toward Developing a Security Policy*, 12 J. MARSHALL J. COMPUTER & INFO. L. 425 (1993) (arguing that current law can accommodate electronic documents created and maintained in adequately secure environments). The costs associated with legislative endorsement of one particular technology (public-key encryption technology, or, more narrowly, specific implementations of this technology) and whether this endorsement will affect the development of alternative solutions to the problems posed by communications over open computer networks deserve consideration. A wide variety of approaches to electronic commerce have developed without government intervention; perhaps current law and market forces can solve the problems posed by the Internet without ambitious new legislation. *See, e.g.*, WRIGHT, *supra* note 3, § ET1.3.2 (describing the online payment system of First Virtual Holdings, Inc.), § ET3.1 (describing Mondex electronic cash), § ET3.2 (describing First Bank of the Internet), and Appendix G (describing the Pen-Op system of capturing handwritten signatures electronically). *See also The Quick Tour; A Summary of Approaches; Electronic Commerce Industry Overview*, RELEASE 1.0, Jan. 24, 1995, at 6. There are other cost-related issues: the institutional overhead associated with creating and maintaining the Act's infrastructure will be passed along to participants, and participants must have access to expensive computer hardware and software in order to participate in the system. The Utah Act does not address the question of whether citizens who are unable to afford these costs should be provided with subsidized or reduced-cost access to the infrastructure. Universal service provisions in telecommunications law may prove instructive.

signatures are held to a standard of reasonable care in preventing disclosure of their private encryption key.[121] In contrast to the carefully articulated duties the Act requires of certification authorities, the Utah Act is virtually silent when it comes to determining what constitutes reasonable care on the part of subscribers in safeguarding their private keys. Thus, this issue of what constitutes reasonable care will be shaped by the expensive and often inelegant process of court decisions gradually determining a standard. In the long run, a sensible, workable standard may emerge from this process. In the meantime, however, this lack of a clear standard could lead to inconsistent decisions by courts struggling to understand a complex, emerging technology, and lead to inequitable results for those unable to marshal the considerable resources necessary to make complicated, technology-based arguments before a tribunal which may be ill-equipped to understand the relevant issues.

The problems with the ill-defined standard of care imposed on subscribers in safeguarding private keys are compounded by the evidentiary presumptions imposed by the Utah Act. In adjudicating disputes involving digital signatures, the Utah Act instructs courts to presume (among other things) that if a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority, (i) the subscriber has accepted the corresponding certificate (and thus assumed the duty to exercise reasonable care to protect the relevant private key), (ii) the digital signature is the digital signature of the subscriber listed in the certificate, and (iii) the digital signature was affixed with the intention of signing the message.[122] Thus, if a subscriber is defrauded by a criminal who somehow obtains that subscriber's private key and uses it to commit fraud, the subscriber must come to court with evidence which rebuts this presumption. That is, the subscriber challenging a fraudulent digital signature must come to court with evidence showing that they in fact did not affix the digital signature in question, and that they exercised reasonable care in protecting their private key. Moreover, it appears that under Utah law this presumption shifts to the subscriber not only the burden of producing prima facie evidence to rebut the presumption, but also the burden of persuading the finder of fact that the presumed facts are not true.[123] Indeed, because

---

121. § 46-3-305(1).
122. § 46-3-406(3).
123. Utah law distinguishes between presumptions which shift the burden of persuasion on an issue and those which shift only the burden of making a prima facie case on the matter. *See, e.g., In re* Swan's Estate, 293 P.2d 682 (Utah 1956) (some presumptions are not eliminated upon the introduction of prima facie evidence but have the effect of placing on the disfavored party the burden of persuading the factfinder that the facts are contrary to the presumed facts). *See generally* William E. Shipley,

digitally signed documents are considered acknowledged documents under the Utah Act, the burden may be an onerous one. Clear and convincing evidence is generally required of the party asserting the invalidity of an acknowledgment; a mere preponderance of the evidence is not sufficient.[124]

To illustrate the difficulties that the allocations of liability and evidentiary burdens under the Utah Act pose for subscribers who utilize digital signatures under the Act, consider the following hypothetical, adapted from an example provided by the drafters of the Utah Act:[125]

> Cedric, a licensed certification authority, duly issues a certificate to Susan, who accepts it. Cedric publishes the certificate in a recognized repository. Susan's private key, which corresponds to the public key in the certificate, is kept on a floppy disk. Irving, a malicious computer hacker, releases a computer virus on the Internet that finds its way onto Susan's computer. Subsequently when Susan uses her private key, the virus program surreptitiously sends a copy of Susan's private key to Irving. Irving immediately uses the private key to cash a $10,000 electronic check drawn upon Susan's account payable to a numbered, anonymous account in a state having rigorous bank secrecy laws. Irving disappears and cannot be found. As soon as Susan learns of the fraud she revokes her certificate.

Annotation, *Effect of Presumption as Evidence or Upon Burden of Proof, Where Controverting Evidence is Introduced*, 5 A.L.R.3d 19 (1966). Whether or not a presumption falls into one category or another is a complicated question of law, and an analysis of whether the presumptions of the Utah Act would, by themselves, shift the evidentiary burden will not be attempted here. The issue is likely moot because of the "acknowledged document" status the Utah Act provides digitally-signed documents. Regardless of whether the presumptions alone would shift the evidentiary burden to a subscriber, because digitally-signed documents are acknowledged under the Utah Act a subscriber attacking the validity of a digitally-signed document bears a substantial evidentiary burden. *See* note 124, *infra*, and accompanying text.

124. 1 AM. JUR. 2D *Acknowledgments* § 84 (1994). This issue is discussed in Part V(B), *infra*.

125. Adapted from an illustration provided in UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 91-92. The illustration provided therein had Irving stealing a floppy disk containing Susan's private key from Susan's purse. It is interesting to note that none of the illustrations provided by the drafters of the Utah Act include the scenario where a private key is captured by a computer virus, even though the Digital Signature Legislative Facilitation Committee considered this possibility. In a memo to the Committee, Alan Asay wrote, in the context of discussing a CA's private key: "if the certification authority's system security has been breached without the certification authority's knowledge (such as by a virus that has compromised the certification authority's private key), the certification authority must revoke." Memorandum from Alan Asay to the Digital Signature Legislative Facilitation Committee, Sept. 23, 1994 (copy on file with author.)

According to the analysis of this scenario provided by the drafters of the Utah Act, under the Act Susan will be liable for the loss caused by the forgery if she failed to exercise reasonable care in safeguarding her private key.[126] The Act provides no guidance as to whether the failure to protect one's computer from a virus constitutes a breach of the duty of reasonable care. Thus, Susan must obtain the services of an attorney well-versed in computer technology and go to court. Susan must overcome the presumption that the electronic check signed with her digital signature is valid and binding upon her. The electronic check will have the status of an acknowledged document, so clear and convincing evidence is required to challenge its validity. Susan must show that in fact she did not affix the digital signature in question. Furthermore, she must show that she did not breach her duty of care in allowing Irving, the criminal, to obtain her private key. If Susan is unsuccessful after this time-consuming and expensive process, then Susan will bear the $10,000 loss.

The allocations of liability and evidentiary burdens imposed by the Utah Act put users of digital signatures who are victimized by fraud in a position that is disadvantageous compared to several analogous situations. Consumers who participate in the infrastructure developed under the Utah Act subject themselves to a far greater risk of liability than they face in other electronic transactions, such as credit card or debit card transactions. The liability allocations and evidentiary burdens of the Utah Act contradict the spirit, and in certain circumstances (such as the example of Susan and Irving, *supra*) the letter, of consumer-protection statutes such as the Electronic Fund Transfer Act (EFTA)[127] and the Truth in Lending Act.[128] Moreover, a defrauded consumer challenging the practice of a certification authority in court faces more difficult evidentiary burdens than a defrauded consumer challenging the practice of a notary. The liability allocations and burdens of proof imposed by the Utah Act most closely resemble the law relating to telecommunications "toll fraud," which itself has been highly controversial. A comparison follows of the liability provisions of the Utah Act to these three analogous models, the "credit card model," the "notary model," and the "toll fraud model." Proposed reforms in the arena of toll fraud suggest an alternative liability allocation scheme that would more effectively protect the interests of all participants in a public key

126. UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 92.
127. 15 U.S.C. §§ 1693-1693r (1994).
128. 15 U.S.C. §§ 1601-1667e (1994).

system and promote the development of a robust public key infrastructure.[129]

A. The "Credit Card Model"

A comparison of the liability allocations and evidentiary burdens of the Utah Act to the liability provisions of two federal consumer protection statutes, the Electronic Fund Transfer Act and the Truth in Lending Act, proves instructive. The virtually identical liability schemes of these two Acts will be termed the "credit card model," at the risk of being somewhat misleading. The combined scope of these two Acts is much broader than just credit card transactions, but for the purposes of comparison with the Utah Act, the focus will be on the provisions of these Acts which address consumer liability in credit card-like electronic transactions. An analysis of this legislation demonstrates, first, that some transactions using digital signatures will fall under the purview of at least the EFTA, and the liability scheme of the Utah Act will be preempted for a certain narrow class of transactions. More broadly, the

---

129. The potential magnitude of the fraud problem in the context of a public key infrastructure is completely unknown. In other contexts the fraud problem is enormous. In 1994 Mastercard reported a loss of $486 million due to credit card fraud; Visa's fraud loss was $645 million. Robert Jennings, *Fraud is Stealing Holiday Joy from Credit Card Companies*, AM. BANKER, Dec. 7, 1995, at 1. The number of consumers who are victims of "true name fraud" or "identity theft" has been skyrocketing. In 1993, the credit reporting agency Trans-Union received an average of 300 calls per month to their fraud line set up for victimized consumers; by February of 1996 they were receiving 1200 calls *per day*. *60 Minutes* (CBS television broadcast, Feb. 25, 1996). According to AT&T, telecommunications toll fraud costs American businesses $2 billion annually. *Carriers, PBX Makers, Customers Debate Toll Fraud Responsibility*, REP. ON AT&T, Feb. 14, 1994, *available in* LEXIS, NEWS Library, ZTL1 File. Phone companies estimate that they lose about $3 billion to calling card fraud and other types of fraud. Peter Sinton, *Visa Has Sights Set on Credit Card Fraud*, S.F. CHRON., Sept. 14, 1994, at B1. Interestingly, the preventative efforts of at least one group of telecommunications companies, the Regional Bell Operating Companies (RBOCs) or "Baby Bells," have been directed "almost exclusively" at calling card fraud, even though this type of fraud represents only 12 percent to 15 percent of overall phone fraud. *Local Telcos Slow Joining Industry Fight Against Phone Fraud*, TELCO BUS. REP., May 22, 1995, *available in* LEXIS, NEWS Library, NWLTRS File. *See also Local Phone Companies Found to be Apathetic Toward Security*, 12 COMM. DAILY 1, *available in* LEXIS, NEWS Library, NWLTRS File. As mentioned in note 132, *infra*, under the Truth in Lending Act, consumer liability for calling card fraud is generally capped at $50, and thus the RBOCs bear a substantial portion of the losses caused by calling card fraud. However, customers are strictly liable for other types of telecommunications fraud, as discussed in Part V(C), *infra*, and the RBOCs bear virtually no risk of loss for this kind of fraud.

EFTA and the Truth in Lending Act demonstrate a strong federal policy in favor of consumer protection which the Utah Act simply ignores. This analysis is not intended to assert that the liability allocations of the EFTA and Truth in Lending Act necessarily should govern in a public key infrastructure. Indeed, as explored further below, some differences exist between the credit card model and a public key infrastructure which may justify different liability rules.

Certain transactions utilizing digital signatures will likely be governed by the liability rules of the Electronic Fund Transfer Act. Consumers' rights in this class of transactions contrast sharply with the rights that the Utah Act provides to consumers in transactions that are not preempted by the EFTA. To illustrate the potential applicability of the EFTA to transactions utilizing digital signatures, reconsider the hypothetical involving Susan and Irving, introduced *supra*. According to the analysis provided by the drafters of the Utah Act, Susan will likely be liable for the loss caused by the forgery if she failed to exercise reasonable care in safeguarding her private key. While this may be true as far as the Utah Act goes, this analysis fails to consider the applicability of the EFTA, which, under this scenario, would likely preempt the Utah Act and limit Susan's liability to $50 and impose the bulk of the loss upon the financial institution, as well as shift the burden of proof in any dispute away from Susan and onto the financial institution.

The EFTA was enacted for the purpose of providing a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems, and its primary objective is the provision of individual consumer rights.[130] Electronic fund transfer is defined in the EFTA as "any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer . . . so as to order, instruct, or authorize a financial institution to debit or credit an account."[131] The EFTA limits a consumer's liability for unauthorized electronic fund transfers to, in most cases, $50.[132] The

130. 15 U.S.C. § 1693(b) (1994). *See also* 12 C.F.R. § 205.1(b) (1996). The purposes of the EFTA are to be carried out by regulations prescribed by the Board of Governors of the Federal Reserve System. 15 U.S.C. § 1693b(a) (1994). The regulations adopted by the Board are known as "Regulation E" and are found at 12 CFR 205.1 to .14 (1996).

131. 15 U.S.C. § 1693a(6) (1994).

132. A consumer's liability for an unauthorized electronic fund transfer is capped at the *lesser* of $50 or the aggregate amount of unauthorized transfers occurring prior to the time that the consumer gives notice to the financial institution, unless the consumer 1) fails to report unauthorized transfers appearing on a periodic statement within 60 days (absent extenuating circumstances), or 2) fails to report loss or theft of a card or other means of account access within two business days (absent extenuating

liability limits of the EFTA apply if the "access device used for the unauthorized electronic funds transfer is an accepted access device."[133] An "access device" is defined as a "card, code, or other means of access to a consumers account, or any combination thereof, that may be used by the consumer for the purpose of initiating electronic funds transfers."[134] It is an "accepted access device" when the consumer to whom the access device was issued "[r]equests and receives . . . or uses . . . the access device for the purpose of transferring money between accounts or obtaining money, property, labor, or services."[135] In any action which involves a consumer's liability for an unauthorized fund transfer, the burden of proof is on the financial institution to establish that the conditions set forth in the EFTA, which allow application of the EFTA's liability provisions, are met.[136]

The applicability of the EFTA in the Susan/Irving scenario may turn upon the question of whether the technology used to affix a digital signature constitutes an "access device." Significantly, the Information Security Committee's Digital Signature Guidelines assert that it does not:

> A private key, as defined in these Guidelines, is not an "access device" within the meaning of 12 C.F.R. § 205(2)(a)(1) (1994) (Regulation E of the Board of

---

circumstances), in which case liability is capped at the lesser of $500 or the amount of actual loss. 15 U.S.C. § 1693g (1994). The provisions in the Truth in Lending Act that concern credit cards address liability issues in largely the same fashion. *See* 15 U.S.C. § 1643 (1994). The EFTA was strongly influenced by the Truth in Lending Act. *See* Roland E. Brandel & Eustace A. Olliff III, *The Electronic Fund Transfer Act: A Primer*, 40 OHIO ST. L.J. 531, 537 (1979) (noting that the EFTA "borrows concepts and techniques for legal control" from the Truth in Lending Act, as well as from other legislation such as the Fair Credit Billing Act, 15 U.S.C. §§ 1666-66j (1994), and the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994)). One difference in the liability provisions of the Truth in Lending Act and the EFTA is that the Truth in Lending Act caps consumer liability in all circumstances at $50. As under the EFTA, under the Truth in Lending Act a card holder's negligence is irrelevant to the issue of liability, and the card issuer bears the burden of proof on authorization. 15 U.S.C. § 1643(b) (1994). In addition to applying to traditional credit cards, the Truth in Lending Act's liability provisions apply to utility credit cards, such as those supplied by a phone company and used to procure telecommunications services. *See, e.g.*, Chartways Technologies, Inc. v. AT&T Communications, 6 F.C.C.R. 2852, 2954 (1991). Thus, when a customer's calling card is used fraudulently, that customer's liability is limited to $50. The Truth in Lending Act does not apply to the type of telecommunications toll fraud discussed *infra*, Section V(C).

133. 12 C.F.R. § 205.6(a)(1) (1996).
134. 12 C.F.R. § 205.2(a)(1) (1996).
135. 12 C.F.R. § 205.2(2)(i) (1996).
136. 15 U.S.C. § 1693g(2)(b) (1994).

> Governors of the Federal Reserve System), but rather, a private key is a device for creating a digital signature, which satisfies a requirement of a signature as provided in Guideline 5.1 [which states that legal signature requirements are satisfied by a digital signature which meets certain specifications]. Therefore, loss of a private key is not governed by the provisions of Regulation E concerning the loss of an access device, *see* 12 C.F.R 205.6 (1994) [which, among other things, limits consumer liability for unauthorized fund transfers].[137]

This assertion is ultimately unpersuasive, however. The plain language of the EFTA's "access device" definition would include many forms of digital signature technology, although perhaps not literally the private encryption key itself. In the Susan/Irving scenario, Susan stored her private key on a floppy disk. An alternative method for storing a private key would be on a credit card-like "smart card." In either case, the disk or card and the information stored on the disk or card would appear to fall within the realm of a "card, code, or other means of access to a consumers account, or any combination thereof, that may be used by the consumer for the purpose of initiating electronic funds transfers." In a 1994 work analyzing the possible implementation of a federal certification authority (FCA), Michael Baum, who chairs the committee which issued the Digital Signature Guidelines, discusses the potential applicability of the EFTA to digital signature technology under certain circumstances. Baum describes how "the FCA may issue certificates, or FCA-users may hold their private keys and/or create digital signatures using a card technology in a form analogous to traditional credit, debit, or automated teller machine ('ATM') cards."[138] Baum cites an interview with a U.S. Treasury Department representative who notes that "[i]f the FCA is implemented using card technologies, [portions of] such card usage would probably be interpreted as coming under the purview of Reg. E."[139] Baum's proposals concerning an FCA assume the non-involvement of consumers, "[b]ecause of the added complexity and risks typically imposed on the providers of consumer products and services."[140] Addressing the larger policy issue, Baum notes that

---

137. DRAFT DIGITAL SIGNATURE GUIDELINES, *supra* note 118, § 4.3.5.

138. MICHAEL S. BAUM, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY 262 (1994). This 388 page (plus appendix), extensively footnoted book provides a comprehensive survey of the wide array of legal issues implicated by a proposed federal certification authority, and is highly recommended as a resource for anyone interested in the legal issues surrounding the implementation of a public key infrastructure. It is published by the U.S. Department of Commerce's National Technical Information Service as Report No. PB94-191202.

139. *Id.* at 267.

140. *Id.* at 18.

> consumer protection legislation in the payment systems area can be viewed as a means for consumers to deal with organizations, systems, and processes that are somehow 'beyond' them. To the extent that the establishment of the FCA would constitute a radical departure from existing practices, similar protections may be appropriate for even sophisticated business concerns.[141]

The argument that the EFTA would preempt the Utah Act and apply to some transactions which use digital signatures is buttressed by the broad consumer-protection mandate the law provides the Federal Reserve Board. This broad mandate also highlights the importance of the consumer-protection policy which underlies the Electronic Fund Transfer Act. The EFTA confers broad authority[142] on the Board to prescribe regulations to further the EFTA's primary objective of providing individual consumer rights.[143] The Board's authority is a function of whether funds transfers are initiated electronically, whether current laws provide adequate consumer safeguards, and whether coverage under the EFTA is necessary to achieve the EFTA's basic objectives.[144] Congress contemplated that, as no person can foresee electronic fund transfer developments, "regulations would keep pace with new services and assure that the [EFTA's] basic protections continue to apply."[145] Thus, in "the event that electronic fund transfer services are made available to consumers by a person other than a financial institution holding a consumer's account, the Board shall by regulation assure that the disclosures, protections, responsibilities, and remedies created by this title are made applicable to such persons and services."[146]

In the absence of new regulations from the Federal Reserve Board, however, many types of transactions that would utilize digital signatures would fall well outside the purview of the EFTA. The EFTA thus does not comprehensively replace the liability allocations of the Utah Act through preemption. The EFTA would not be applicable to any

---

141. *Id.* at 239.

142. "This provision [15 U.S.C. § 1693b(c), which defines some duties of the Board] is virtually identical to section 105 of the Truth in Lending Act, a provision interpreted by the United States Supreme Court as granting the Board great discretion in defining coverage. The Court consistently has recognized the Congress' delegation of broad authority to the Board." 58 Fed. Reg. 8714, 8715-16 (1993).

143. 15 U.S.C. § 1693(b) (1994).

144. 58 Fed. Reg. 8714, 8715 (1993).

145. S. REP. NO. 95-915, 95th Cong., 2d Sess. (1978) *reprinted in* 1978 U.S.C.C.A.N. 9403, 9412.

146. 15 U.S.C. § 1693b(4)(d) (1994).

transaction not involving a "consumer" and a "financial institution."[147] Digital signatures could be used for many activities other than electronic fund transfers, such as signing contracts or filing legal documents. If a particular fraudulent transaction utilizing digital signatures involves a consumer, a financial institution, and an electronic fund transfer, the EFTA will dramatically limit the consumer's liability and place the burden of proof in any consequent dispute upon the financial institution. If a consumer is victimized in a fraudulent transaction which does not include an electronic fund transfer, or which does not involve a financial institution, the Utah Act's liability scheme will apply and that consumer will be subject to potentially unlimited liability unless that consumer can prove that they in fact did not affix the digital signature in question, and that they exercised reasonable care in protecting their private key. Even assuming that the liability scheme imposed by the Utah Act is more appropriate than that of the EFTA because of unique problems posed by digital signature technology, the interaction of the Utah Act and the EFTA will create, in addition to a complex and confusing legal landscape for consumers, a skewed certification authority industry. That is, financial institutions, which would otherwise be likely candidates for the role of certification authority and frequent users of digitally-signed electronic documents, would face dramatically different litigation costs and liability exposure than other entities involved in the Utah Act's digital signature scheme.

Digital signature technology does involve some unique risks, and the credit card model embodied in the EFTA and in the Truth in Lending Act does not provide a perfect fit as a model for liability allocation in a public key infrastructure. The credit card model differs from a public key infrastructure in at least two important ways. First, the consequences of consumer negligence in a public key infrastructure are arguably more significant than the consequences of consumer negligence in the credit card model. The success of a public key infrastructure depends upon the security of private keys. If consumers faced a maximum liability of $50 for unauthorized transactions which utilized their private key, a "moral hazard" problem is created.[148] That is, consumers may lack the financial incentive to take adequate steps to keep their private

147. The term "consumer" means natural person. 15 U.S.C. § 1693a(5) (1994). The term "financial institution" means a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person who, directly or indirectly holds an account belonging to a consumer. 15 U.S.C. § 1693a(8) (1994).

148. *See generally* READINGS IN THE ECONOMICS OF CONTRACT LAW 2 (Victor P. Goldberg ed., 1989).

key secure, and may in fact have the incentive to commit fraudulent acts. Of course, this same problem exists under the credit card model as well.[149] Proponents of heightened liability in the digital signature context argue that virtually the only way that fraud involving digital signatures can occur is if a holder of a private key somehow discloses it,[150] whereas fraud in the credit card context can occur in a number of different ways, including many that involve no fault on the part of the credit card holder. This argument is partly flawed.[151] Nonetheless, the general point that the security of private keys is critical to the functioning of a public key infrastructure is true, and this fact may justify some differing treatment of consumers in a digital signature context in contrast to the credit card model. It is not clear, however, that this difference justifies the extensive liability exposure that the Utah Act imposes on consumers in contrast to the liability policies embodied in the EFTA and the Truth in Lending Act.

A second way in which the credit card model diverges from the reality of a public key infrastructure concerns the availability of a "deep pocket" entity able to act as a *de facto* insurer. Under the credit card model, financial institutions absorb the costs of fraud and redistribute these costs to all of their customers in the form of higher fees, higher interest rates, per-use charges to merchants, and the like. In a public key infrastructure, certification authorities could conceivably play this role. However, unlike financial institutions, certification authorities may not be able to limit their liability exposure by accepting as customers only those who the CA determined were credit-worthy. Moreover, while the

---

149. In the credit card context this problem, to the degree that it is one, is mitigated somewhat by the extensive costs imposed upon victimized consumers apart from the $50 liability cap (which is, in practice, often waived). Consumers who are fraud victims must expend considerable time and effort correcting erroneous information on credit reports, filing police reports, etc. *See, e.g.*, Marcia Vickers, *Stop, Thief! And Give Me Back My Name*, N.Y. TIMES, Jan. 28, 1996, § 3, 1. *See also* PRIVACY RIGHTS CLEARINGHOUSE, COPING WITH IDENTITY THEFT: WHAT TO DO WHEN AN IMPOSTOR STRIKES (1996) (pamphlet produced by San Diego, CA-based consumer group). In light of the difficulties victimized consumers face, consumers have considerable incentive to keep their credit cards secure.

150. "[A] person is quite powerless to prevent forgery of her paper signature, but, in all but rare instances, only a subscriber can prevent the most likely cause forged digital signatures, by keeping the private key safe." UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 20.

151. See the discussion concerning the implementation of public key cryptographic algorithms in Part V(C).

recommended reliance limit on a certificate would limit the CAs' liability in any single transaction, no analogy to the credit card limits imposed by financial institutions exists for transactions involving certificates and digital signatures. Nor would CAs profit from each transaction in which a subscriber engaged, as financial institutions do with credit cards. Many transactions utilizing digital signatures may not be financial transactions at all. Additionally, the kinds of fraud that occur under the credit card model can often best be prevented by vigilance on the part of the financial institution (that is, the financial institution is often the "cheapest cost avoider"[152]), whereas in a public key infrastructure the holder of a private key, rather than the certification authority, is arguably best positioned to prevent many types of fraud.

In sum, the liability model embodied in the EFTA and in the Truth in Lending Act may not translate effectively to the realm of digital signatures. There are two important lessons to be learned from these consumer protection statutes, however. First, regardless of whether its policies are better or worse than the very different liability policies of the Utah Digital Signature Act, the EFTA will apply on its own force to certain kinds of transactions which utilize digital signatures, thus undermining the comprehensiveness of the Utah Act's liability scheme. Second, the EFTA and the Truth in Lending Act illustrate a wide-ranging federal policy in favor of consumer protection. The Utah Act ignores consumer protection as an important policy consideration. By doing so, it not only opens itself up to broader federal preemption, but also undermines its ostensible goal of promoting the development of a public key infrastructure. Consumers will not utilize a system which subjects them to potentially unlimited liability.

B. The Notary Model

Notaries Public provide a model for liability allocation and allocation of evidentiary burdens that can be instructively contrasted to the scheme set out in the Utah Act. Some of the activities performed by certification authorities are analogous to the activities of notaries. The critical function of a certification authority in a public key infrastructure is to correctly identify a potential subscriber and issue a certificate which assures others of the subscriber's identity. Likewise, in witnessing or attesting a signature, the acquisition of evidence that the subscriber is

152. *See generally* GUIDO CALABRESI, THE COST OF ACCIDENTS 135-40 (1997).

who he or she purports to be is an essential part of the full and faithful execution of a notary's duty.[153]

The "notary model" appears to have been a model which was actively contemplated by the drafters of the Utah Act. Some of the terminology used in the Utah Act is similar to language used to describe various elements of notarial practice. The person who appears before a notary is a "subscriber."[154] Notarial acts must be evidenced by a "certificate" signed and dated by a notarial officer.[155] The Utah Act imposes record-keeping requirements on certification authorities that are not unlike those typically imposed on notaries.[156] The bonding requirements imposed on CAs by the Utah Act are similar to the bonding requirements commanded of notaries.[157] Under the Utah Act documents signed with certain digital signatures are given a legal status similar to that of notarized documents.[158]

In taking and certifying an acknowledgment, notaries are required to act with the care and diligence that reasonably prudent and cautious persons exercise under like circumstances.[159] That is, notaries are held to a negligence standard. Thus, a notary is liable to all persons who have been defrauded of money as a result of relying upon the genuineness of a document executed by the notary in performance of his or her official duties. However, a notary is not a guarantor or an insurer, and if the notary is to be held liable at all, it must be on the ground of negligence (or intentional wrongdoing).[160]

In an action to recover against a notary for failure to adequately perform required duties, generally the burden is on the plaintiff to prove the notary's negligence and show the consequent harm.[161] However, if the duty breached is the notary's duty to exercise reasonable care in

153. 58 AM. JUR. 2D *Notaries Public* § 32 (1989).
154. *Id.*
155. UNIFORM LAW ON NOTARIAL ACTS § 7(a), 14 U.L.A. 136 (1982).
156. *Compare* UTAH ADMIN. R. 154-10-303 (1996) (regulations prescribing record-keeping practices of certification authorities) *with* 58 AM. JUR. 2D *Notaries Public* § 40 (1989) (record keeping requirements of notaries).
157. *Compare* Utah Act §§ 46-3-103(34)(a), -104(3)(b) *and* UTAH ADMIN. R. 154-10-201 (1996) (provisions relating to a certification authority's suitable guaranty) *with* 58 AM. JUR. 2D *Notaries Public* § 74 (1989) (describing liability of a surety on a bond issued for a notary).
158. § 46-3-405.
159. 1 AM. JUR. 2D *Acknowledgments* § 117 (1994).
160. 58 AM. JUR. 2D *Notaries Public* § 58 (1989).
161. *Id.* § 60.

establishing a subscriber's identity when taking an acknowledgment, the evidentiary burden shifts to the notary to establish that the proper standard of care was exercised once a plaintiff establishes that the acknowledged signature is forged.[162] Shifting the burden of persuasion to the notary once forgery has been determined is justified by the probability that the notary was negligent in ascertaining the identity of the forger and by the strong public interest in ensuring the accuracy of notarial certifications.[163]

The Utah Digital Signature Act imposes a standard of care on certification authorities that is similar to the negligence standard imposed on notaries, but with some significant qualifications. The Utah Act provides that certification authorities shall not be liable "for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with all the material requirements of this chapter."[164] That is, the certification authority who complies with the duties articulated elsewhere in the Act enters a "safe harbor," sheltered from any risk of liability. The requirements imposed elsewhere in the Act are, in many instances, similar to the duties required of a notary under a negligence standard. For example, a certification authority must confirm the identity of prospective subscribers[165] and confirm that the information in a certificate to be issued is accurate,[166] as well as engage in other, unique duties such as ensuring that a prospective subscriber holds a private key capable of creating a digital signature.[167] In contrast to the more amorphous negligence standard imposed on notaries, the question of whether a certification authority has satisfied a required duty can usually be answered by a "bright line" test.

The notary model shifts the burden of persuasion in a dispute over a forged acknowledgment or signature once the forgery has been shown. That is, once a plaintiff shows that a signature is forged, the burden shifts to the notary to prove that the notary exercised the proper standard of care. The Utah Digital Signature Act contains no similar provision. Thus, a person challenging the practice of a certification authority faces

---

162. *Id.* § 66. Similarly, where the failure of a notary's identification of a subscriber is established, and consequently the falsity of the notary certificate, the burden of persuasion shifts to the notary to show a deception perpetrated through no lack of reasonable care. *Id.*

163. *Id.*

164. § 46-3-309(2)(A).

165. § 46-3-302(b)(i).

166. § 46-3-302(b)(iii).

167. § 46-3-302(b)(v).

much more difficult evidentiary burdens than a person challenging the practice of a notary.

A proponent of the scheme embodied in the Utah Act might argue that this sort of burden-shifting would be inappropriate in the digital signature context in light of the policies behind burden-shifting in the notary model: the probability that the notary was negligent is ascertaining the identity of the forger and the strong public policy of ensuring the accuracy of notarial certifications. These policies arguably carry less force when applied to certification authorities. Fraud can easily occur in the absence of negligence on the part of the CA because, for example, a criminal could discover a subscriber's private key long after a CA dutifully identified that subscriber and issued a certificate, and therefore, placing this burden on a CA does not further the policy of ensuring accurate certifications. This argument most effectively makes a much broader point, however: the notary model is not a useful model to apply to a public key infrastructure.

The activities of a certification authority and a notary are fundamentally different, despite superficial similarities. Both the certification authority and the notary engage in a process of identification. The activities of a notary, however, focus on a particular instrument or transaction. A person appears before a notary, document in hand. The notary confirms this person's identity, and issues a written certificate that states that the person who executed the instrument to which the certificate is attached was known to, and appeared before, the notary and acknowledged the instrument to be his or her voluntary act.[168] The acknowledged instrument is then generally admissible into evidence without further proof of its execution, and the burden is upon the person challenging its contents to prove his contention by clear and convincing evidence. Evidence must be "clearly cogent and convincing beyond any reasonable controversy" in order to impeach a notary's certificate.[169]

A subscriber generally appears before a certification authority once. The CA identifies the subscriber and issues that subscriber a certificate containing the public key which corresponds to the private key retained by that subscriber. Subsequently, a subscriber can produce an unlimited number of electronic documents, all of which will be verified by the same original certificate. The Utah Act states:

---

168. 1 AM. JUR. 2D *Acknowledgments* § 1 (1994).
169. 58 AM. JUR. 2D *Notaries Public* § 43 (1989).

> [A] certificate issued by a licensed certification authority is an acknowledgment of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgment appear with the digital signature or whether the signer physically appeared before the certification authority when the digital signature was created, if that digital signature is: (1) verifiable by that certificate; and (2) affixed when that certificate was valid.[170]

Thus, documents signed with digital signatures are acknowledged documents. The commentary to this portion of the Utah Act notes the applicability of Utah Code section 78-25-7, which states that "the certificate of . . . acknowledgment . . . is prima facie evidence of the execution of [a] writing."[171] The annotations accompanying this statute indicate that the effect of a certificate of acknowledgment "will not be overthrown upon a mere preponderance of the evidence," but rather "the evidence must be clear and convincing."[172] Thus, despite the fact that documents are not certified individually in the personal presence of a notary as they are under the notary model, all instruments signed with digital signatures are acknowledged documents and achieve a difficult-to-challenge legal status. The notary model is taken too far. Digitally-signed documents do not achieve the same assurances of genuineness that documents signed in the personal presence of a notary achieve, and should not be given the same legal status. Providing digitally-signed documents with this status creates unreasonable evidentiary burdens for victims of fraud challenging the validity of electronic documents signed with the victim's private key.

C. The Telecommunications Toll Fraud Model

The liability allocations and evidentiary burdens imposed by the Utah Act perhaps most closely resemble the law concerning telecommunications toll fraud. Toll fraud entails a third party "hacker" gaining remote access to a private branch exchange (PBX)[173] and placing unauthorized

---

170. § 46-3-405.

171. UTAH CODE ANN. § 78-25-7 (1992).

172. *Id.* (citing Northcrest, Inc. v. Walker Bank & Trust Co., 248 P.2d 692 (Utah 1952)).

173. A PBX is comprised of sophisticated switching equipment which allows businesses with many employee telephones to have station-to-station dialing, direct dialing to each station from outside the business premises, and a single directory number for the business – all without the need to route calls through an attendant. CHARLES H. KENNEDY, AN INTRODUCTION TO U.S. TELECOMMUNICATIONS LAW 24 (1994). In the telecommunications lexicon, PBXs are one type of Customer Premises Equipment (CPE). Thus the type of fraud under discussion is sometimes termed CPE fraud.

long distance calls that are billed to the owner of the system.[174] The magnitude of the resulting fraud can be enormous. For example, the non-profit San Ysidro Health Center, which serves a low-income clientele near the Mexican border just south of San Diego, received a bill for $82,000 in fraudulent calls.[175] AT&T sued San Ysidro Health Center to compel payment of this bill.[176] Under the law applicable to telecommunications toll fraud, calls "originate" at a customer's number when calls, authorized or not, are made from that customer's telephone system.[177] Customers from whose number a call originates are strictly liable for that call, regardless of whether the call was placed fraudulently.[178]

Advocates of this system of liability argue that the customer is the party with the ability to prevent fraud from occurring, and thus imposing liability on the customer creates incentives to minimize fraud. The PBX owner has primary care, custody, and control of the PBX equipment, and thus can best take preventative steps to eliminate fraud.[179] This liability scheme and its underlying rationale have proven controversial. One commentator notes that "[f]ew telecommunications issues in recent years have created more concern . . . than the PBX toll fraud problem."[180]

Critics of the PBX toll fraud liability scheme point out that other parties, in addition to the PBX owner, are well-positioned to prevent fraud. Long distance companies can take steps to prevent fraud. One company that suffered $300,000 in toll fraud losses noted that in one month their "800" number usage jumped from 100 calls to over 10,000, and their international calls jumped from a few hours per month to "thousands" of hours. Their long distance carrier, AT&T, did not inform them of any problem; the victimized company learned of the fraud when

174. Thomas K. Crowe, *Companies at Risk from Toll Fraud*, CORP. LEGAL TIMES, Apr. 1993, at 39.

175. Joe Cantelupe, *$82,000 Phone Bill Has Shrill Ring At Health Center*, SAN DIEGO UNION-TRIB., April 15, 1995, at B1.

176. *Id.*

177. AT&T v. Jiffy Lube Intl., Inc., 813 F. Supp. 1164, 1167 (D. Md.) (citing Chartways Technologies, Inc. v. AT&T Communications, 6 F.C.C.R. 2852 (1991)).

178. *See generally Businesses Pay for Toll Fraud*, TELECOMM. ALERT, Feb. 5, 1996, *available in* LEXIS, NEWS Library, NWLTRS File.

179. REP. ON AT&T, *supra* note 129, at 2.

180. Thomas K. Crowe, *Long Distance Services Theft: Who Pays?*, NAT. L. J., Oct. 19, 1992, at 19.

they received the bill.[181] Similarly, the manufacturers of PBX equipment can prevent fraud, by building security functions into the PBX equipment and teaching customers to use these functions, and by alerting customers to potential risks concerning the equipment which they otherwise might not be made aware. Because long distance companies and PBX equipment manufacturers face little liability risk, however, they have little incentive to take these prudent steps.[182]

Like the law of telecommunications toll fraud, the Utah Digital Signature Act places a significant risk of liability on a subscriber/customer, with the rationale that the subscriber is best positioned to prevent fraud (by safeguarding the subscriber's private key) and thus will have the appropriate incentives to do so. In the toll fraud arena, the liability standard imposed on customers is strict liability. Under the Utah Digital Signature Act, the standard imposed on subscribers is, ostensibly, a negligence standard. As discussed *supra*, however, the burden on a subscriber who is attacking a fraudulently signed digital document is an onerous one. If a hacker breaks into a subscriber's computer system, gains access to a subscriber's private key, and creates a large number of facially valid but fraudulent electronic documents, that subscriber will face enormous practical hurdles in challenging those electronic documents. Thus, for many subscribers, particularly those who lack the resources necessary to pursue their rights in court, the Utah Act imposes a *de facto* strict liability standard.

The telecommunications toll fraud model is effective as an analogy for a public key infrastructure in some respects because it introduces an actor who is ignored in the Utah Act and in the credit card model and notary model considered *supra*: the equipment manufacturer. The hardware and software used to create digital signatures is a critical weak point in the framework of a public key infrastructure. While the Utah Act empowers the Division of Corporations and Corporate Code to "review software for use in creating digital signatures and publish reports concerning software,"[183] the Act is otherwise silent on the issue of the duties of equipment manufacturers.

Cryptographic algorithms are at the core of a public key infrastructure. For these algorithms to fulfill their promise, it is absolutely essential that

---

181. *Complaints on Toll Fraud Aired at FCC En Banc Hearing*, COMM. DAILY, Oct. 13, 1992, at 1, *available in* LEXIS, NEWS Library, NWLTRS File.

182. See *supra* note 129.

183. § 46-3-104(3)(c). The 1995 version of the Act empowered the Division to "approve asymmetric cryptosystems for use in signing certificates issued by licensed certification authorities," and to issue rules addressing the "suitability of algorithms for use in fulfilling the requirements of this chapter." UTAH CODE ANN. §§ 46-3-501(4), -501(5)(c) (Supp. 1995) (repealed 1996).

they be implemented correctly. This is not an easy task. For example, the Netscape Navigator World Wide Web browser uses the RSA public key algorithm for encryption. A criminal who wanted to decrypt a message encrypted using Netscape's system and who didn't have the key would, theoretically, need a supercomputer and thousands of years in order to decipher it. However, in September of 1995, two Berkeley graduate students discovered a flaw in Netscape's implementation of the RSA algorithm, which allowed them to decrypt encrypted messages in a matter of seconds.[184] Similarly, in March of 1996 a security flaw in the Java programming language was announced, a flaw which would allow an attacker to surreptitiously add and remove data from the computers of visitors to a Web site which exploited the flaw.[185] This flaw conceivably would allow a criminal to capture a visitor's private key, as described in the Susan/Irving hypothetical, *supra*. A theoretical virus-born attack on the private keys of PGP users has been announced on the Cypherpunks mailing list.[186] The implementation of cryptographic algorithms is a difficult and risky process.[187]

The liability allocations of the Utah Act can be subject to the same criticism that has been directed at the liability rules embodied in the law of toll fraud. Subscribers bear an immense amount of risk under the Utah Act. If electronic documents are fraudulently signed with a subscriber's digital signature, that subscriber faces a substantial possibility that he or she will bear any resulting loss. To some degree, a subscriber can prevent fraud by taking steps to safeguard the subscriber's private key. However, a private key can be discovered in ways that are totally outside the control of a subscriber. Generating key pairs, for

---

184. Bill Orr, *The Netscape Debacle: Healthy Wakeup Call?* AM. BANKERS ASS'N BANKING J., November 1995, at 74. *See also* Levy, *supra* note 21.

185. Don Clark, *Researchers Find Big Security Flaw in Java Language*, WALL ST. J., Mar. 26, 1996, at B4.

186. E-mail message from Bill Frantz to C. Bradford Biddle (Feb. 22, 1996) (describing PGP attack developed by Frantz and noting that a description of the attack had been posted to the Cypherpunks list, archived at <http://www.hks.net/cpunks/>) (printed copy on file with author). For general information about PGP, see GARFINKEL, *supra* note 52. For more information about the Cypherpunks, an informally-organized group dedicated to defending privacy with cryptography, anonymous electronic mail forwarding systems, digital signatures, and electronic currency, visit the list archives.

187. Another example of the difficulties inherent in implementing encryption schemes can be found in *First Virtual Holdings Identifies Major Flaw in Software-Based Encryption of Credit Cards; Numbers Easily Captured by Automated Program*, PR NEWSWIRE, February 7, 1996, *available in* LEXIS, NEWS Library, NWLTRS File.

example, is a notoriously tricky process. If the hardware or software used to generate key pairs is flawed, private keys could be easily discovered.[188] In the context of toll fraud, one toll fraud victim said "PBX owners should not be responsible for 100 percent of the toll fraud if we don't control 100 percent of our destiny."[189] The same principle applies in a public key infrastructure. The heavy burden of liability which the Utah Act places on subscribers is inappropriate in light of the fact that there is a substantial likelihood of fraud occurring which is not the result of a subscribers negligence, but instead based on faulty hardware or software. Some measure of liability risk should explicitly be placed on hardware and software providers in order to ensure that adequate care is taken to prevent this sort of fraud.

D. A Proposal Based on Unenacted Toll Fraud Reforms

The law of telecommunications toll fraud has been roundly criticized, and reform efforts have been launched on several fronts. In 1993, the Federal Communications Commission (FCC) issued a Notice of Proposed Rulemaking (NPRM) designed to address toll fraud problems.[190] This rulemaking effort appears to have stalled. In 1992, the Telephone Toll Fraud Remedies Act (TTFRA) was introduced in Congress.[191] The TTFRA was not enacted, but it nonetheless provides an instructive alternative to liability allocation in the world of toll fraud, and thus can serve as a model for liability allocation in a public key infrastructure.

The TTFRA was designed to achieve two purposes: (1) to prevent toll fraud by requiring PBX equipment makers and sellers to adequately warn customers about the possibility of toll fraud, inform customers about the appropriate precautions to take to prevent such fraud, and alert customers to the risk of financial exposure they assume when purchasing PBX equipment; and, (2) to provide a mechanism for adjudicating toll fraud liability disputes.[192] The TTFRA provided that disputes involving allegations of toll fraud be subject to arbitration at the option of a

---

188. *See supra* notes 21 and 183.
189. REP. ON AT&T, *supra* note 129.
190. Policies and Rules Concerning Toll Fraud, 58 Fed. Reg. 65,153 (1993) (proposed Dec. 13, 1993). Among other things, this NPRM noted that the FCC had "tentatively concluded that carrier tariff provisions that historically have placed strict liability on customers that are victims of toll fraud without acknowledging any obligation by the carriers to warn customers of risks of using carrier services are unreasonable." *Id.* at 65,154.
191. H.R. 6066, 102d Cong., 2d Sess. (1992).
192. *Id.* § 3.

customer (and not at the expense of the customer).[193] The Act emphasizes timely resolution of disputes.[194] The arbitration would involve the customer, the common carrier, and the equipment manufacturer or dealer.[195] The TTFRA called upon the FCC to develop security guidelines for use by customers in guarding their PBX equipment.[196] Presumably a customer who adhered to these guidelines would avoid liability for negligence. If a customer was found to be negligent, they would be held liable for the loss caused by the fraud. The TTFRA is silent concerning burdens of proof and sufficiency of evidence.

Many of the principles of the TTFRA can be applied in the context of a public key infrastructure. The Act's emphasis on adequate warnings certainly translates to the realm of digital signatures. Subscribers must be informed by their hardware or software provider about steps that they should take to adequately protect their private keys, and must be informed about the liability exposure that they face when participating in a public key infrastructure. The TTFRA's dispute resolution mechanism may translate to the world of digital signatures as well. Subscribers who challenge a digital signature as fraudulent could have the opportunity to immediately appeal to an arbitrator or "expert agency" with expertise in electronic transactions. If that subscriber can show that they did not affix the digital signature in question (the evidentiary burden here should certainly be lower than "clear and convincing evidence") and that they adhered to clearly articulated guidelines in protecting their private key, then that subscriber should not bear the full brunt of the loss.

The recipient of a facially valid digitally-signed document should not necessarily fully bear the loss either; otherwise, reliance on digitally-signed documents will be chilled and the benefits of a public key infrastructure lost. Instead, the arbitrator could apportion the loss between the hardware/software provider, the repository, the certification authority, and the subscriber, depending on relative degree of fault. If a software system is cracked, for example, enabling the fraud, then the software provider should be liable. Likewise if a CA or a repository causes a loss, they should be responsible.

---

193. *Id.* § 4(b)(6), 4(b)(6)(B).
194. *Id.* § 4(d).
195. *Id.* § 4(b)(6).
196. *Id.* § 4(b)(3).

One difficult question arises when no entity is clearly at fault; that is, when subscriber, CA, recipient, software/hardware provider, and repository all perform as well as can reasonably be expected, and yet a loss still occurs. In such a situation the loss should fall on the recipient, the party that chose to rely on the fraudulent digitally signed message. This party is best able to assess the risks associated with relying on any particular message. If the potential risk of loss is high, this party can make "out of band" contacts (i.e., telephone or in-person contacts) with the ostensible sender to obtain assurances about the authenticity of the message, or can choose not to rely on the message at all.

Another difficult question arises when a consumer-subscriber, after being provided specific, understandable guidelines concerning how to protect his or her private key, fails to comply with those guidelines, resulting in a substantial loss. Having a consumer bear potentially unlimited liability does not comport with the policy of consumer protection embodied in the EFTA and Truth in Lending Act. Furthermore, consumers may not choose to participate in the infrastructure if they are potentially subject to unlimited liability, although the force of this argument is reduced if the guidelines with which a consumer must comply in order to avoid liability are clear and reasonable (thus making the risk of unlimited liability low). Perhaps the best approach in this scenario is to simply cap consumer liability, even for negligent failure to comply with the applicable guidelines, at a fixed amount in a fashion similar to the EFTA. The amount should be much higher than the $50 limit in the EFTA—perhaps $1000—or perhaps could be tiered based on the degree of fault—i.e., $500 for "ordinary negligence," $2500 for "gross negligence," $5000 for "recklessness" and no limit for intentional wrongs. While this approach will potentially impose unreimbursed losses on parties who rely on digital signatures, presumably parties would take this into account in their risk-benefit calculus when choosing to rely on a digital signature. In a large dollar transaction, the relying party may choose to obtain out of band assurances. In a small dollar transaction, the relying party may simply choose to accept this risk of loss.

Insurance should eventually address the problem of unreimbursed losses. A private insurance market will not develop immediately, however, because of the lack of a pattern of loss experience and other factors.[197] In the meantime, the proposal outlined above could provide parties participating in a public key infrastructure with a reasonable

197. BAUM, *supra* note 138, at 338.

degree of certainty, enabling them to make rational economic choices, without abandoning the policy of consumer protection.

E. A Liability Cap for Certification Authorities?

Turning back to the public key infrastructure actually implemented by the Utah Digital Signature Act, a final criticism of the Act's liability provisions is in order. The Utah Act provides a *de facto* liability cap for certification authorities, which under easily-envisioned circumstances will preclude complete recovery for numerous innocent defrauded parties. This policy decision will undermine the integrity of the infrastructure the Act is designed to promote.

It is easy to envision a scenario in which a CA's private key is compromised. One way that this could occur is through brute force cryptanalysis: a "factoring attack."[198] That is, a criminal could simply dedicate the immense amount of computing power needed and "break" the underlying algorithm, discovering a CA's private key from an analysis of the CA's public key. Alternatively, a criminal could threaten, blackmail, or torture an employee of the certification authority, forcing the employee to surrender the CA's private key, a process described as "rubber hose cryptanalysis."[199] The criminal could bribe a CA employee: a "purchase-key attack."[200] An incompetent employee could simply reveal the key accidentally. A flaw in the hardware and software utilized by the CA could be discovered and exploited.

The compromise of a CA private key could be catastrophic. A publication from RSA Laboratories notes that "[i]t is extremely

198. At the risk of immensely oversimplifying the issue, the mathematical premise behind public key cryptography is that it is easy to multiply two prime numbers to get a third number, but it is very difficult to "factor" that third number and recover those two primes. Generating a key pair involves multiplying two large primes. Figuring out a private key from a public key involves factoring a large number. If the number (or "key length") is large enough (i.e., 300 digits or more), one expert estimates it would take more than $300 trillion in computing resources to determine a private key from a public key. SCHNEIER, E-MAIL SECURITY, *supra* note 7, 45-46, 49. Public key cryptographic algorithms are often implemented with relatively short key lengths because of export restriction imposed by the U.S. Government, however, and can be broken through a "brute-force" attack. *See* Levy , *supra* note 21, at 134, 196-200 (describing the successful effort to break the export version of Netscape Navigator's 40-bit encryption key).

199. SCHNEIER, APPLIED CRYPTOGRAPHY, *supra* note 7, at 7.

200. *Id.*

important that private keys of certifying authorities are stored securely because compromise would enable undetectable forgeries."[201] A criminal who discovers the private key of a certification authority could produce an unlimited number of ostensibly valid certificates. The criminal could enter into fraudulent transactions under a host of assumed names, or could create certificates in the name or particular individuals or corporations and impersonate those individuals or corporations electronically. Moreover, once a CA's private key was compromised and the corresponding public key revoked, all certificates issued by that CA would be invalid. All of the subscribers who utilized that CA would be forced to obtain new certificates.[202] The costs associated with a compromised CA key dramatically outweigh the costs associated with a compromised subscriber key.

A criminal with a certification authority's private key could cause an immense amount of financial damage, imposing huge losses on a number of innocent parties. These innocent parties would be unable to recover their full losses from a negligent certification authority if the total of these losses was greater than the amount of that certification authority's "suitable guaranty." A suitable guaranty is either a surety bond or an irrevocable letter of credit that meets certain administrative specifications[203] and is designed to facilitate recovery of any judgment obtained against a CA. The Utah Division of Corporations and Commercial Code is empowered to determine an amount appropriate for a suitable guaranty in a rulemaking proceeding, in light of the burden a suitable guaranty places upon licensed certification authorities and the assurance of financial responsibility it provides to persons who rely on certificates issued by licensed certification authorities.[204] The Act states that "[a]

---

201. RSA FAQ, *supra* note 7, § 3.8.
202. *Id.* § 3.10.
203. § 46-3-103(34)(a).
204. § 46-3-104(3)(b). The 1995 version of the Utah Act did not delegate this power to the rulemaking process, and instead set out a formula for calculating the amount of a suitable guaranty in the statute itself. UTAH CODE ANN. § 46-3-103(34)(A)(II) (Supp. 1995) (repealed 1996) provided that the amount of the suitable guaranty be the greater of either (a) 100% of the largest recommended reliance limit of any certificate issued by a certification authority, or (b) 35% of the total recommended reliance limits of all certificates issued by a certification authority. Recommended reliance limits are dollar figures specified in a certificate which indicate the certification authority's liability and financial responsibility limits in transactions using that certificate. UTAH CODE ANN. § 46-3-103(26) (Supp. 1995) (repealed 1996); 1996 Utah Laws § 46-3-103(28). This issue was discussed at the October 3, 1995 meeting of the Utah Digital Signature Legislative Facilitation Committee. The minutes to this meeting note:

> The definition of "suitable guaranty" was discussed extensively. Mr. [David W.] Moore [representing Utah Title and Escrow School] stated that the cost of the bond or letter of credit required by the suitable guaranty provision may

suitable guaranty may also provide that the total annual liability on the guaranty to all persons making claims based on it may not exceed the face amount of the guaranty."[205] Financial institutions acting as certification authorities are exempted from the requirement of posting a suitable guaranty.[206]

If a defrauded subscriber obtains a judgment against a certification authority, they can recover that judgment plus attorney's fees from the CA's suitable guaranty.[207] However, the total liability on the suitable guaranty to all persons making claims upon it cannot exceed the amount of the suitable guaranty.[208] Thus, in the easily-envisioned scenario of widespread fraud caused by a CA's compromised private key, defrauded subscribers may not be able to recover the full amount of their losses from the negligent CA. The CA's liability is effectively capped at the amount of their suitable guaranty. All of the defrauded subscribers may be able to obtain judgments against the CA. However, no rational businessperson entering the CA business would organize the business in such a manner as to create liability exposure beyond that required by the suitable guaranty. The CA will do business in a corporate form which will make the CA essentially judgment-proof in the event of catastrophic widespread fraud based on a compromised private key.[209] There are no other financial responsibility provisions in the Utah Act, and thus the suitable guaranty will serve as a liability cap.

The risk of a compromised certification authority private key is a very serious risk in a public key infrastructure. Because the rewards from

---

> eliminate title companies from the market since their product guarantees the validity of a mortgage. He suggested setting a less onerous standard by Administrative Rule. Mr. [Alan] Asay [representing the Utah Division of Corporations] . . . stated that the percentages expressed in this Subsection are not based on industry track records because no such record exists . . . . Mr. Asay suggested amending the suitable guaranty amount to half of what is currently stated in the law. Mr. [Michael] Wims [of the Utah Attorney General's Office] made a motion that the amount of the bond or letter of credit be established by Administrative Rule. This motion passed unanimously.

Minutes of The Utah Digital Signatures Act Legislation Facilitation Committee (October 3, 1995) (copy on file with author).

205. § 46-3-103(34)(b).

206. § 46-3-103(34)(c).

207. § 46-3-310. It is unclear whether a subscriber could collect attorney's fees in an action against a financial institution serving as a CA.

208. § 46-3-310(2).

209. For a summary of how the corporate form can serve to limit liability, see ROBERT W. HAMILTON, FUNDAMENTALS OF MODERN BUSINESS §§ 13.6, 13.8 (1989).

successfully obtaining a CA's private key could be great, criminals will likely expend considerable resources trying to obtain the private keys of CAs. CAs must guard their private keys with extreme vigilance. Capping the CA's liability when the CA negligently discloses their private key is an undesirable public policy. If a certification authority does not have to potentially bear the full costs of any losses resulting from a compromised private key, they may not have the incentive to take expensive precautions to protect against that occurrence.[210]

The rationale of the drafters of the Utah Act in limiting the liability of CAs is, presumably, to foster development of a certification authority industry.[211] Assuming that this is a worthy goal, capping CAs' liability does not accomplish it effectively.[212] As noted, CAs will not have adequate incentives to take expensive precautions to protect their private key. Moreover, the CA who is negligent will be able to externalize the costs of their negligence onto otherwise innocent defrauded subscribers and other parties. A more sensible approach would be to require all CAs to insure against this type of catastrophe. The discipline of an insurance market would promote appropriate investment on the part of the CAs in light of the relevant risk.

A private insurance market may not develop immediately,[213] although faced with the prospect of numerous CAs required to purchase expensive insurance coverage it is certainly possible that a competitive insurance industry could quickly develop an appropriate insurance package. In the meantime, perhaps the state could temporarily act as an insurer, creating an insurance pool from proceeds collected from all CAs. The passage of digital signature legislation indicates that state legislatures have determined that the development of a public key infrastructure is beneficial to the public. The perceived benefits of a public key infrastructure may warrant state involvement to promote the development of a private sector insurance pool, in order to maximize preventative steps taken to avoid a serious risk, and to guarantee recovery for innocent public key infrastructure participants in the event of CA negligence.

---

210. *See generally* Calabresi, *supra* note 152.

211. *See, e.g.*, UTAH DIGITAL SIGNATURE LAW, *supra* note 1, at 58: "As with any other business enterprise, a certification authority must be able to assess and manage its risk of exposure to potential liability, and one of the principal impediments to the emergence of certification authorities has been the uncertainty of the legal risks such a business would undertake."

212. The liability cap imposed by the Utah Act can be criticized as a subsidy designed to foster development of a favored industry. *See generally* MORTON J. HOROWITZ, THE TRANSFORMATION OF AMERICAN LAW 1780-1860 (1977).

213. BAUM, *supra* note 138, at 338.

VI. CONCLUSION

The liability provisions of the Utah Digital Signature Act create an attractive legal environment for the entrepreneur contemplating a business as a certification authority. If a CA complies with explicitly defined rules, they enter a safe harbor, sheltered from liability. Even if the CA fails to comply with these rules and negligently imposes losses on large numbers of subscribers, the CA enjoys a *de facto* liability cap. The drafters of the Utah Act evidently believe that, with legal risks so clearly defined, entrepreneurs will rush to enter the CA market, creating a public key infrastructure, which, presumably, will benefit all who participate in it. This view must be questioned. Consumers who participate in the infrastructure developed under the Utah Act subject themselves to extensive liability risk compared to a variety of analogous situations, and face difficult evidentiary burdens in resolving disputes which arise under the Act. Consumers will not participate in a system that subjects them to such dramatic risks. Moreover, by limiting the liability of CAs to an amount which is less than the actual damages a certification authority can cause, the economic integrity of the infrastructure is weakened. The Utah Digital Signature Act manifests misplaced priorities. Promoting the development of a public key infrastructure is a worthwhile goal. However, it should not be accomplished by abandoning the policy of consumer protection embodied in the EFTA and other federal legislation, nor should it be accomplished by encouraging development of a system which allows enterprises to externalize the costs of their negligence, thus producing a less-than-robust infrastructure. Indeed, by ignoring the policies of consumer protection and economic integrity, the Utah Digital Signature Act may ultimately undermine development of the infrastructure that the Act is ostensibly designed to promote.

C. BRADFORD BIDDLE