Notes on PKI and Digital Negotiability: Would the Cybercourier Carry Luggage

Walter Effross

Follow this and additional works at: https://digitalcommons.wcl.american.edu/facsch_lawrev

Part of the Computer Law Commons, and the Law and Economics Commons
NOTES ON PKI AND DIGITAL NEGOTIABILITY: WOULD THE CYBERCOURIER CARRY LUGGAGE?

Walter A. Effross*


"It has often been said that a negotiable promissory note is a courier without luggage whose face is its own passport."

"To be negotiable, a note must be a courier without luggage; it must move unencumbered."

Traditionally, commercial law has insisted that negotiable instruments encapsulate an obligation or order of payment in a pure and streamlined form. In an era increasingly marked by electronic rather than paper-based negotiation, the Uniform Commercial Code as revised in 1990 continued this policy by

---

* Walter A. Effross is Associate Professor, Washington College of Law, American University, and Chair of the American Bar Association’s Subcommittee on Electronic Commerce. © Walter A. Effross 1998.


3. U.C.C. art. 3 Prefatory Note (1995) (all references in this Note are to the 1995 version of the U.C.C.) (taking into account the transition from "a paper-based system ... to modern technologies now employed and the procedures required by the current volume of checks").

4. Id. (observing that "Revised Article 3 may, not inappropriately, be regarded as the latest effort in the progressive codification of the common law of negotiable instruments that began with

SPRING 1998 385
requiring, for instance, that a negotiable instrument be “payable on demand or at a definite time”\textsuperscript{5} and “not state any other undertaking or instruction by the person promising or ordering payment to do any act in addition to the payment of money.”\textsuperscript{6}

However, these changes did not address the possibility of electronic forms of non-check drafts and notes. This Article explores the manner in which public key infrastructure (“PKI”) technology could be applied to enhance a system of electronic or “digital” negotiable instruments other than checks.\textsuperscript{7} Does it even make sense, for instance, for Alice to write a promissory note to Bob in the form of an e-mail? How could Bob indorse it to Connie and negotiate it to her? How could the parties be sure that signatures were not forged or the terms of the instrument altered?

Part I of the Article provides a brief summary of the operation of PKI and its use of certification authorities. Part II summarizes the relevant elements of negotiability and the forms of negotiable instruments under Article 3 of the Uniform Commercial Code. Part III examines the application of PKI technology to support a system of digital negotiability and raises the problem of the fraudulent computerized “cloning” of such instruments.

I. PUBLIC KEY INFRASTRUCTURE AND CERTIFICATION AUTHORITIES

Public key cryptography as a method for protecting the confidentiality, integrity, and authenticity of messages has significant advantages over the more familiar forms of security involving such “symmetric single keys” as passwords or personal identification numbers. As one leading commentator has observed, in symmetric single key systems the sender (say, Alice) and the recipient (say, Bob) must trust each other not to reveal the password or “key,” which is used to both encrypt and decrypt the message, thereby weakening “non-repudiation”; that is, Alice may be able to deny that the message came from her by admitting that she had compromised the secrecy of the key by accusing Bob of having compromised it. Alice and Bob must also resort to a different key or an entirely different secure method in order to communicate this password initially to each other or to a third party (Connie) so that she can use their original key.\textsuperscript{8}

\textsuperscript{5} Id. § 3-104(a)(2).
\textsuperscript{6} See id. § 3-104(a)(3).
\textsuperscript{7} Article 4 of the Uniform Commercial Code addresses the specialized collection process for checks.
\textsuperscript{8} See Charles R. Merrill, \textit{Proof of WHO, WHAT and WHEN in Electronic Commerce under the Digital Signature Guidelines} 503 PLI/Pat 119 (1997); Charles R. Merrill, \textit{Cryptography: The
An asymmetric public key system removes this problem by providing each participant with her own "key pair," consisting of a secret "private key" as well as a publicly available "public key." These keys, strings of alphanumeric characters, are mathematically linked to each other in such a way that they are complementary "toggle switches," but that it is "computationally unfeasible to derive the secret key from the public key." 9

To encrypt a message so that it could be deciphered only by Bob, Alice (or any other party) would obtain Bob's public key and use a public-key algorithm, to send it to Bob, who would decrypt it by applying his private key to the message. If another party, David, received or intercepted this e-mail message it would be unintelligible to him because he could not, even knowing Bob's public key, discover Bob's private key.

An especially elegant feature of this system is its use to authenticate, or "digitally sign," documents. That process is the reverse of the one above: to digitally sign an electronic document that she is sending to Bob, Alice would apply her private key to the entire message 10 or to a "digest" of it. 11 When Bob receives the message, he can decrypt it using Alice's public key; and since no one but Alice should have Alice's private key to digitally sign it, Bob can use Alice's public key to verify that the message came from Alice. Moreover, because the signed form of the message incorporates not only information about the signer but information about the content of the message itself, if the signed message has been tampered with en route to Bob, his attempted verification of it using Alice's

9. Cryptography, supra
10. See Closen & Richards, supra note 8, at 735 (observing that "[the signature itself] is actually a "hash"—a string of digits (letters, numbers, and/or symbols) representing a combination of the document and the unique computer-generated code produced by the document's signer" and that this signature, which is unique to each document signed, is generated by the signer's typing a personal identification number or phrase into the encryption program); see also Cryptography, supra note 8, at 8 (noting that "every character in the message is verified because the software runs the contents through a one-way hash algorithm that digitally signs the hash.").

11. See Biddle, supra note 8, at 1149 (indicating that the sender "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.").
public key should fail. Thus, the digital signature process also assures Bob of the integrity of the message.\(^\text{12}\)

Of course, Alice could combine the two processes if she is concerned that her digitally signed message will be intercepted by someone other than Bob. If the message is not encrypted for confidentiality by Alice, then the unauthorized recipient can read it, can verify to himself and to a third party that Alice signed it and that it was not altered since the time it was signed by Alice. To protect against this, Alice could also encrypt for confidentiality her digitally signed message (the one prepared using her private key) with the public key of the recipient, Bob. Then, only Bob would be in a position to decrypt it, and thus to read it and to verify to himself and to a third party that it had come to him unaltered from Alice. We will explore below in Part III how such precautions could also prevent an unauthorized recipient from negotiating a digitally signed message to an unsuspecting third party.

How, though, can Alice be sure that in sending a message to Bob she has Bob's correct public key, or Bob be sure that in decrypting Alice's message he has Alice's correct public key instead of one of an impostor? To resolve this problem, public key systems have added "certification authorities" ("CAs") to vouch for the proper match of party with public key (and thus with the unique private key that corresponds to the public key).\(^\text{13}\) CAs provide parties with "certificates" that, in essence, corroborate one or more characteristics of the person to whom the certificate is issued—in this case, the party's identity and public key. Such certificates are digitally signed by the CA.\(^\text{14}\)

---

12. See Closen & Richards, supra note 8, at 736 (discussing this benefit of public key encryption); see also Froomkin, supra note 8, at 54 (noting that "because the signature uses the original text as an input to the encryption algorithm, if the message is altered in even the slightest way, the signature will not decrypt properly, showing that the message was altered in transit or that the signature was forged by copying it from a different message.").

13. See Cryptography, supra note 8, at 9 (characterizing certification authorities as "a kind of DNA binding the public key to the owner's identity"); see also Closen & Richards, supra note 8, at 737 (characterizing certification authorities with "cybernotaries"); Froomkin, supra note 8, at 55 (defining a certification authority generally as "a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing digital certificates that attest to some fact about the subject of the certificate.").

14. See Froomkin, supra note 8, at 58 (defining a certificate as "a computer-based record which: (1) identifies the CA issuing it, (2) names, identifies, or describes an attribute of the subscriber, (3) contains the subscriber's public key, and (4) is digitally signed by the CA issuing it."). One commentator has described a form of procedure by which certificates might be issued:

Alice would generate her public and private key pair. She would then take her public key (on a floppy disk [or her laptop], 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 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.

Biddle, supra note 8, at 1150-51.
II. NEGOTIABLE INSTRUMENTS AND NEGOTIABILITY

Article 3 recognizes two types of negotiable instruments: drafts and notes. Each of these types meets the general definition of a negotiable instrument as "an unconditional promise or order to pay a fixed amount of money, with or without interest or other charges described in the promise or order [that is]; (1) payable to bearer or to order at the time it is issued or first comes into possession of a holder; (2) is payable on demand or at a definite time; and (3) does not state any other undertaking or instruction by the person promising or ordering payment to do any act in addition to the payment of money. . . ."15

An instrument is a "note" if it is a "promise,"16 itself defined as "a written undertaking to pay money signed by the person undertaking to pay."17 An instrument is a "draft" if it is an "order,"18 or "written instruction to pay money signed by the person giving the instruction."19

An electronic message whose content conforms to the criteria above (for instance, "I, Alice Adams, promise to pay $5.00 to Bob Basin or his order on December 1, 1998.") would thus seem to have only two hurdles to overcome: being a "writing" and being "signed." The current version of the Uniform Commercial Code defines both of these concepts quite broadly, to encompass elements far beyond the colloquial meaning of these words.20

III. USES OF PKI FOR DIGITAL NEGOTIABILITY

A. Digital Signatures

Determining who signed an instrument is crucial for purposes of fixing liability under Article 3: a person is not liable on an instrument unless he or an agent or representative with the power to bind him signed it.21 Moreover, someone applying to an instrument an "unauthorized signature" (i.e., one that

15. U.C.C. § 3-104(a).
16. See id. § 3-104(e).
17. Id. § 3-103(a)(9).
18. See id. § 3-104(e).
19. Id. § 3-103(a)(6). A "check" is a special type of draft, "payable on demand and drawn on a bank" or "a cashier's check or teller's check." Id. § 3-104(f).
20. A "writing" includes "printing, typewriting or any other intentional reduction to tangible form." Id. § 1-201(46). It is "signed" if it contains any "symbol . . . executed or adopted by [a] party with present intention to authenticate [a] writing." Id. § 1-201(39).
21. See id. § 3-401(a). See also id. § 3-402(a) (providing that "[i]f a person acting, or purporting to act, as a representative signs an instrument by signing either the name of the represented person or the name of the signer, the represented person is bound by the signature to the same extent the represented person would be bound if the signature were on a simple contract," and that "[i]f the represented person is bound, the signature of the representative is the 'authorized signature' of the represented person and the represented person is liable on the instrument.").
does not bind his purported principal) may be personally liable on the instrument.  

Although the Uniform Commercial Code does not specifically address electronic communications, its underlying principle of commercial flexibility has led the drafters of revisions to Article 2 and of a new article dealing with the licensing of information to propose that the more expansive concept of a "record" be substituted for the traditional "writing." In addition, Draft Article 2B provides that "[a] record or authentication may not be denied legal effect, validity, or enforceability solely on the ground that it is in electronic form."

However, Articles 1 and 3 of the Uniform Commercial Code do not yet recognize explicitly the effect of electronic documents and digital signatures made through the PKI process. Such revisions would greatly promote the establishment of digital negotiability. Not only would PKI signatures enable parties to avoid forgeries, but many practical questions of a signer's authority to bind her purported principal to liability on a negotiable instrument could be averted if a CA certified, in addition to the correspondence between the signer's identity and the signer's public key, the relevant scope of the signer's authority to bind various parties. The person to whom the instrument was offered could check the signer's authority with the CA.

In practice, the recipient of a signed and encrypted digital negotiable instrument would decrypt it with his private key, add to the decrypted version his

---

22. See id. § 3-403(a) (providing that generally "an unauthorized signature is ineffective except as the signature of the unauthorized person in favor of a person who in good faith pays the instrument or takes it for value").

23. See id. § 1-102 cmt. 1 (indicating the drafters' intent "to make it possible for the law embodied in [the U.C.C.] to be developed by the courts in light of unforeseen and new circumstances and practices").


26. The term "digital signature" is commonly used to refer to signatures made through the use of a private key. By contrast, an "electronic signature" is a much broader concept, including not only digital signatures but names or symbols typed into an e-mail message, whether or not those have the security protections of signatures made with private keys. See Uniform Electronic Transactions Act § 102 (8) (Proposed Draft Mar. 23, 1998) <http://www.law.upenn.edu/library/ulc/uecta/cta398.htm> (broadly defining an "electronic signature" as "any signature in electronic form, attached to or logically associated with an electronic record").
indorsement or other information, and then digitally sign the new document using his private key. Under existing Article 3 provisions, anyone who transfers an instrument for consideration warrants, unless he disclaims such warranties, that "all signatures on the instrument are authentic and authorized"; nonetheless, to ensure that subsequent recipients of an encrypted instrument could confirm that the prior signatures were authentic, a person might, before transmitting the encrypted instrument by e-mail, attach to that electronic mail message (as an unencrypted separate document, digitally signed with his own private key) a copy of the message that he had received.

That is, if Alice were to send Bob an electronic mail message that constituted a promissory note payable to Bob or his order, she would sign it using her private key and encrypt it with Bob's public key. Bob would decrypt it with Bob's private key, verify Alice's digital signature using Alice's public key, then indorse the decrypted note by digitally signing it with his own private key. Bob could negotiate this indorsed note to Connie by transferring "possession" of it to her by e-mail, attaching a file containing Alice's decrypted note. To verify Alice's signature as maker, Connie would use Alice's public key on Bob's attachment (the decrypted message that Alice sent to Bob), and to verify Bob's signature as indorser Connie would use Bob's public key on Bob's message to Connie.

Although in paper-based transactions makers and drawers usually sign at the lower left corner and indorsers sign on the reverse side, in an electronic context devoid of such reference points, signers should indicate explicitly the capacity of

---

27. U.C.C. § 3-416(a)(2).
28. See id. § 3-201(a) (defining negotiation as "a transfer of possession, whether voluntary or involuntary, of an instrument by a person other than the issuer to a person who thereby becomes its holder"). Under U.C.C. § 1-201(20), a "holder" of an instrument is "the person in possession if the instrument is payable to bearer or, in the case of an instrument payable to an identified person, if the identified person is in possession." Id. § 1-201(20).
29. This process might appear to resemble the procedure by which a party can verify a digital signature by validating a certificate chain back to the original certification authority, or "root CA." However, the difference is that a signer of the instrument does not act as a certification authority for any other signer; at best, each signer is only warranting under Article 3 that the prior signatures are authentic and authorized.
30. In fact, U.C.C. § 3-204(a)(iii) specifies that the signature of an indorser can appear anywhere on the instrument: "regardless of the intent of the signer, a signature and its accompanying words is an indorsement unless the accompanying words, terms of the instrument, place of the signature, or other circumstances unambiguously indicate that the signature was made for a purpose other than indorsement." Id. § 3-204 (a)(iii).
their signatures, especially when signing as a maker or drawer,\textsuperscript{31} or when signing as a representative of another person.\textsuperscript{32}

\section*{B. Precluding Theft}

The use of public key technology to sign negotiable instruments would make these instruments less vulnerable to theft than their paper-based counterparts. Even if hacker Henry could intercept a digital negotiable instrument that Alice had digitally signed and encrypted with Bob’s public key, Henry would have to be able to supply Bob’s private key to “open” the instrument, read (and perhaps sign) it, and negotiate it further. Unless Bob has compromised the secrecy of his private key, only Bob should be able to negotiate the instrument sent to him by Alice.

This process might seem secure enough to warrant the sending of “bearer” instruments, that is, those payable to “bearer” or his order, or to “cash,” or that do not state a payee or that are not payable to an identified person.\textsuperscript{33} However, given the risks of “cloning” the instrument (discussed below) and the provisions in Article 3 that allow recovery from indorsers if the instrument is dishonored, a better procedure would be for the maker and any indorser\textsuperscript{3} to make any digital negotiable instrument payable to the order of an identified person—namely, to the order of the person to whom the instrument was next being electronically transmitted, or to her principal.

\begin{itemize}
  \item \textsuperscript{31} See id.
  \item \textsuperscript{32} Under U.C.C. § 3-402(b)(1), a representative signing an instrument on behalf of another party but using her own name can preclude her personal liability on the instrument “[i]f the form of the signature shows unambiguously that the signature is made on behalf of the represented person who is identified in the instrument.” Id. § 3-402(b)(1). On paper-based negotiable instruments, this is often accomplished through a multi-line signature:
  \begin{quote}
    XYZ, INC.
    By: [signature of representative]
    [capacity of representative (e.g. “Treasurer,” “Secretary”), XYZ, Inc.
  \end{quote}
  In the digital environment, even if the representative is using her personal private key, she might continue to adopt this typed form of signature in the electronic mail itself.
  A more comprehensive solution would be for representatives not only to indicate their signature in the e-mail text in this manner, but to use special private keys that were linked to the represented party (who might also serve as the representative’s certification authority) and only used by representatives acting on its behalf.
  \item \textsuperscript{33} See id. § 3-109(a).
  \item \textsuperscript{34} U.C.C. § 3-205(a) provides for a “special indorsement” by which “the indorsement identifies a person to whom [the indorser] makes the instrument payable.” Id. § 3-205(a). For example, Bob could specially indorse Alice’s instrument payable to him by signing “Pay to the order of Connie. Bob,” signing the new message with his private key, encrypting it with Connie’s public key, and sending it to Connie.
\end{itemize}
C. Precluding Forgery or Alteration

By employing the private-key process to sign documents, the parties could, as discussed above, preserve the integrity of the document's contents. In terms of Article 3, they would be preventing (or, more accurately, would be providing themselves with a method to detect) any "alterations," or unauthorized changes in an instrument that affect the obligations of a party.\textsuperscript{35} To indicate that he had made not an alteration but an authorized change,\textsuperscript{36} a party would want to attach to the changed document both a copy of the previous version (which itself might include attachments of prior versions) and his own digital certificate indicating that he had the authority to make those changes.

D. The "Possession" Problem

With paper-based negotiable instruments, the nightmare of a maker\textsuperscript{37} of a note, a drawer\textsuperscript{38} or acceptor\textsuperscript{39} of a draft, or an indorser\textsuperscript{40} of a note or draft is that in attempting to discharge her liability on the instrument she will pay the wrong person: that is, someone not entitled to enforce the instrument.\textsuperscript{41} Such a payment does not discharge the payor, and she remains liable to a party that is entitled to enforce an instrument.\textsuperscript{42}

---

35. U.C.C. § 3-407 defines an "alteration" as "(i) an unauthorized change in an instrument that purports to modify in any respect the obligation of a party, or (ii) an unauthorized addition of words or numbers or other change to an incomplete instrument relating to the obligation of a party." Id. § 3-407(a).

36. For example, U.C.C. § 3-115(a) defines an "incomplete instrument" as "a signed writing, whether or not issued by the signer, the contents of which show at the time of signing that it is incomplete [for example, because it is missing the payee's name or the amount payable] but that the signer intended it to be completed by the addition of words or numbers." Id. § 3-115(a). Under U.C.C. § 3-115(c), "[i]f words or numbers are added to an incomplete instrument without authority of the signer, there is an alteration of the incomplete instrument under Section 3-407." Id. § 3-115(c) (emphasis added). Under the Restatement (Second) of Agency (incorporated into the U.C.C. by U.C.C. § 1-103) the signer could grant such authority deliberately (such as by actual or incidental authority), through apparent authority, or through agency by estoppel. See RESTATEMENT (SECOND) OF AGENCY § 26 (actual authority); § 35 (incidental authority); §§ 8, 27 (apparent authority); § 8B (agency by estoppel) (1957).

37. See U.C.C. § 3-103(a)(5) (defining "maker" as "a person who signs or is identified in a note as a person undertaking to pay").

38. See id. § 3-103(a)(3) (defining "drawer" as "a person who signs or is identified in a draft as a person ordering payment").

39. See id. § 3-103(a)(1)(2) (defining "acceptor" as a drawee (i.e., "a person ordered in a draft to make payment") who has "accepted (i.e., agreed to pay) a draft").

40. See id. § 3-204(a)(b) (defining "indorser" as "a person who makes an indorsement," that is, "a signature, other than that of a signer as maker, drawer, or acceptor, that alone or accompanied by other words is made on an instrument for the purpose of (i) negotiating the instrument, (ii) restricting payment of the instrument, or (iii) incurring indorser's liability on the instrument. . . . ").

41. Under U.C.C. § 3-602(a), "an instrument is paid [and liability of the payor discharged] to the extent payment is made (i) by or on behalf of a party obliged to pay the instrument, and (ii) to a person entitled to enforce the instrument." Id. § 3-602(a).

42. U.C.C. § 3-301 defines "person entitled to enforce" an instrument. Id. § 3-301.
If, as noted above, liability on a negotiable instrument generally follows from a party's signature, entitlement to enforce an instrument (or, to collect on that liability) normally lies with the person possessing the instrument, namely, with a holder of the instrument, or with a nonholder in possession of the instrument who has the rights of a holder. (However, there are some exceptions.) Indeed, negotiation is defined as "a transfer of possession . . . to a person who thereby becomes its holder." For example, suppose that Alice, in exchange for $50 worth of goods that she received from Bob, were to issue to Bob a note payable on demand to him or his order. A short time later, when she comes into possession of $50, she pays Bob this money and considers her obligation on the instrument discharged. Her assumption is not correct if, before she has given Bob the money, he has negotiated the note onwards to Connie: in that situation, Alice's payment would not discharge her because Bob would not qualify as a party "entitled to enforce the instrument." If Connie were to bring the note to Alice after Alice had paid Bob, Alice would still be liable on the instrument to Connie, since Connie is a holder and is therefore "entitled to enforce the instrument."

In practice, the maker, drawer, acceptor, or indorser can protect herself by demanding to inspect the instrument to ensure that its possessor is qualified as a person "entitled to enforce it," and then by requiring him to turn over the instrument upon his receiving payment. There remains, though, a concern that the instrument might have been entirely fabricated or duplicated by the party presenting it for payment, a concern that is only heightened by the ease, speed, and perfection with which digitized documents can be endlessly cloned.

Can the use of PKI reduce or eliminate the risk that a digital negotiable instrument could be "cloned" by a holder? In the example above, for instance, Bob might be tempted to digitally duplicate Alice's electronic note several times and to use each separate note to pay a different debt of his to other parties. Outside of any questions of their ultimate ability to recover from Bob, would any

43. See id. § 3-301(i).
44. See id. § 3-301(ii). Such a situation typically results from the "transfer" of an instrument without a necessary indorsement that would render the transferee a "holder," see supra note 28, and thus qualify the transfer under U.C.C. § 3-201(a) as a "negotiation." See id. § 3-203(a) (providing that "[a]n instrument is transferred when it is delivered by a person other than its issuer for the purpose of giving to the person receiving delivery the right to enforce the instrument."); see also id. § 3-203(b) (providing that "[t]ransfer of an instrument, whether or not the transfer is a negotiation, vests in the transferee any right of the transferor to enforce the instrument. . . .").
45. Under U.C.C. § 3-301(iii), a person not in possession of an instrument may nonetheless qualify as someone entitled to enforce the instrument if she can prove under U.C.C. § 3-309 that she was once in possession of and entitled to enforce the instrument but that the instrument was lost, destroyed, or stolen. Alternatively, under U.C.C. §§ 3-301(iii) and 3-418(d), if an instrument is paid by mistake and the payor recovers payment, the person from whom payment is recovered has rights as a person entitled to enforce the instrument, even if the instrument has not been returned to that person.
46. Id. § 3-201(a).
of the potential recipients of these notes be able to ensure that he or she is being offered by Bob the "true" copy of the note that Alice sent to Bob? And which would be the "true" copy—the first one that Bob sent?47

This problem is only compounded by the notion underlying all of Article 3: that the "holder in due course," who has taken the instrument for value and in good faith and without notice of various claims against or defenses to liability on the instrument,48 is invulnerable to most defenses against another party's liability on the instrument, but not forgery. But again, even if forgery were defined for these purposes as the unauthorized duplication of the entire instrument, how could the forged copy be distinguished from the original?49 Would an unauthorized duplication immediately void any liability of anyone except the forger on all copies? And how would the other parties know?

Although PKI would practically resolve many issues associated with negotiability, until the threat of cloned "couriers without luggage" can be technologically eliminated the electronic negotiable instrument may well remain only a digital dream.

47. This issue arises also in the context of the principles addressed by the Information Security Committee of the American Bar Association's Section of Science and Technology, in its Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce. Guideline 5.5, which addresses "Digitally signed originals and copies," provides that "[A] copy of a digitally signed message is as effective, valid, and enforceable as the original of the message." INFORMATION SECURITY COMMITTEE, SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND ELECTRONIC COMMERCE 88 (1996) [hereinafter DSG].

Comment 5.5.4 to this Guideline specifically notes the exception that "[a] message, however authentic or genuine, is not treated as a negotiable instrument in banking and business practice unless it is also an original. Possession of the original instrument is crucial in determining whether the instrument was issued." Id. at 89. In Comment 5.5.5, the drafters suggest that "[o]ne possible strategy to reduce the risk of multiple payment of digital instruments is a central registry of the original paper instrument under depository control of a trusted third party, with digital endorsements, presentation and other transactions relating to the original document requiring the digital signature of the trusted third party who retains possession of the original instrument." Id. at 90. This approach, however, would undercut the essence of digital negotiability by involving the third party at every step: even if the "courier" still had no luggage, she would at this point be handcuffed to a traveling companion.

The drafters of the DSG ultimately took no position on this issue, noting in Comment 5.5.7 that "[w]hile the matter is still under consideration, at the present time . . . issues [that] are outside the scope of these Guidelines [include] . . . whether any special treatment should be accorded digital documents which are 'negotiable'. . . ." Id.

48. See U.C.C. § 3-302(a)(2). Under § 3-302(a)(1), there is an additional requirement that "the instrument when issued or negotiated to the holder . . . not bear such apparent evidence of forgery or alteration or is not otherwise so irregular or incomplete as to call into question its authenticity." Id. § 3-302(a)(1). Alteration or forgery of a specific signature would be evident through the use of PKI procedures, but a "forgery" that is the duplication of the entire document would not.

49. DSG, supra note 47, at 88 ("A copy of a digitally signed message is as effective, valid, and enforceable as the original of the message.").