UNDERSTANDING DIGITAL SIGNATURES

By Fritz Grupe, Stephen G. Kerr, William Kuebler, and Nilesh Patel

Digital signatures are a technology that allows two parties to validate the authenticity of electronically transmitted information and documents. When added to a document, a digital signature provides some assurance that the document’s sender is the person she purports to be.

Digital signatures allow companies to share data without the fear of disclosing sensitive information to people for whom it is not intended. The technology is also favored by the federal government and large state governments. This has led to wide acceptance within banking, other financial institutions, government, and large enterprises. SAS 94, The Effect of Information Technology on the Auditor’s Consideration of Internal Controls in a Financial Statement Audit, highlights the professional importance of understanding and managing new technologies such as digital signatures. Many observers believe that the rapid growth of B2B e-commerce will favor the adoption of digital signature online assurance procedures, intrusion testing, and other dynamic technology-enabling processes that can better protect online data.

Background

Digital signature technology grew out of a form of public key cryptography commonly known as public key infrastructure (PKI). In public key cryptography, there are two keys: a private key and a public key. When you send a document to someone, you use a private key, kept secret and known only to the sender, to digitally sign the document. When recipients receive the signed document, they use the sender’s public key, which is available to all recipients, to authenticate the document.

A digital signature is superior to a traditional handwritten signature in many ways. A skilled forger can alter the contents of a document with a handwritten signature or move a signature from one document to another. With digital signature technology, any change in a “signed” document causes the verification process to fail.

A third party, usually called a certificate authority (CA), is usually involved in the exchange of keys and enables the entire process. CAs certify public keys by issuing users a digital certificate that contains the user’s identity, public key, and key expiration date.

One basic requirement of an accounting system is a reliable method to identify and validate each transaction. The cost of inadequate validation control can be staggering. For example, check fraud has been estimated to cost U.S. businesses at least $13 billion a year. Internal control procedures must validate the proper authorization of transactions. In addition, adequate documentation supporting transactions needs to be maintained. Online transactions add new complexity to the accountant’s task of ensuring that only individuals with proper authorization are recording such transactions.

Traditional transactions are managed using manually written, preprinted, or electronic forms. This information is then manually transferred to other forms before the information is further processed and finally fed into the company’s general ledger. This transcription is expensive and error prone, and diverts limited resources from services to routine administration. Transcription is not necessary with paperless technology.

Nevertheless, the savings from reduced paperwork and more responsive systems come with increased audit concerns. Accountants must be especially concerned about the accuracy of information when changes to files, transactions, and temporary alterations to recurring processes are regularly made in digital form. The proper use of digital signatures satisfies the internal control needs raised by these new technologies.

Exhibit 1 illustrates the five typical financial transactions in the purchase, payable, payment cycle. Before Step 5 of the transaction, an accounts payable clerk needs to process the payment and verify that supporting documents related to Steps 1 through 4 have been generated and authorized by appropriate personnel. Getting approval from various individuals and verifying their signatures creates costly paperwork. It also increases the costs and time needed to process the

---

**EXHIBIT 1**

**PURCHASE CYCLE**

<table>
<thead>
<tr>
<th>Transaction</th>
<th>Documents Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Issuance of purchase order</td>
<td>Purchase order</td>
</tr>
<tr>
<td>2. Shipment of goods</td>
<td>Packing slip</td>
</tr>
<tr>
<td>3. Receipt of goods</td>
<td>Delivery slip</td>
</tr>
<tr>
<td>4. Invoicing</td>
<td>Invoice</td>
</tr>
<tr>
<td>5. Payment</td>
<td>Check or EFT memo</td>
</tr>
</tbody>
</table>

---

Editors:
Paul D. Warner, PhD, CPA
Hofstra University

L. Murphy Smith, DBA, CPA
Texas A&M University
transaction. This time directly affects productivity.

Digital signatures dramatically reduce the time needed to process transactions. For example, let's look at Company A and Company B, which both use digital signatures. A wants to place an order for goods from B. A first sends B an encrypted (private) purchase order (PO) and its digital signature over the Internet. B must then be able to verify the following in order to process the PO:

- A sent the PO.
- The PO was sent without error or tampering.
- A cannot deny having sent the PO.

B can perform the validation by simply downloading A's public key. Just being able to locate a current certificate for A from a trusted CA tells B that A is a valid entity with which it can enter into a binding business agreement. After verifying the purchase order, B proceeds to fulfill the order and ship the merchandise. B can also then transmit the packing list, proof of shipment, and invoice—all signed with B's digital signature—to A.

When A decrypts the message using B's public key, A can be certain the information originated with B, has not been tampered with during transmission, and is authentic. A may then choose to make an electronic payment to B, using documents authorized with a digital signature. Since the records of all these transactions are electronic, documents can be transmitted within seconds. In addition, international transactions requiring customs documents and clearances can be processed rapidly using digital signatures.

**Accounting and Auditing Opportunities**

Digital signatures provide specific opportunities to improve internal control and the authenticity of data. It is essential that electronic, legally binding documents and transaction records be subject to a trustworthy process of authentication. Without this, expensive duplication of effort will result from technology deployment, and extensive audit testing will be needed to assess data integrity. Exhibit 2 lists the roles of digital signatures in the authentication process.

These security benefits also allow a CFO to capture some cost savings through workflow efficiencies in the accounting department. These savings include:

- Reduced paper and communications costs
- Reduced transaction and administrative costs
- Reduced head count
- Elimination of process steps

The potential savings in using digital signatures go well beyond the purchase, payable, payment cycle. Some other areas to explore are:

- Paperless contracts
- Regulatory reporting to all levels of government
- Legal documents filed with courts
- Bids on auctions
- Real estate purchases
- Legally binding consent
- Human resources functions, such as approval of vacations
- Payroll
- Supply chain transactions.

**Selection of a Certificate Authority**

The widespread availability of digital signatures has led to three concerns for accountants. The first concern is the selection of a reliable CA. Several choices are now available. The Big Four have started issuing digital signatures in partnership with private vendors such as Verisign. The AICPA's Webtrust seal identifies organizations that follow its availability and control principles and meet its require-

---

### EXHIBIT 2
**AUTHENTICATION ATTRIBUTES OF DIGITAL SIGNATURES**

<table>
<thead>
<tr>
<th>Security Need</th>
<th>Definition of Need</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication of Identity</td>
<td>Assures that a person or system is who or what they claim to be. Verification authenticates both the sender and the integrity of a signed information object.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Provides resource access to authorized users while denying resource access to unauthorized users.</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Protects against unauthorized changes in data, whether intentional or accidental. Verifies that an information object has not been altered by another party.</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>Sender cannot deny that he sent the document.</td>
</tr>
<tr>
<td>Auditing</td>
<td>Monitors security features to identify intentional and unintentional misuse of resources, authority, or responsibility.</td>
</tr>
<tr>
<td>Confidentiality or Privacy</td>
<td>Assurance via encryption that no one but the intended recipient can view specified information. Protects against disclosure of information to unauthorized users. Encryption ensures confidentiality when transmitting information over networks or while storing it.</td>
</tr>
<tr>
<td>Availability</td>
<td>Protects against loss of system operation or erroneous assignment of resources as a result of malicious code, false data, request flooding, or penetration attempts.</td>
</tr>
</tbody>
</table>
ments. Companies contemplating the introduction of digital signature technology should look for such endorsements before choosing a CA.

**Keeping Up With the Law**

A second concern is the rapidly developing legal environment that bears on technology use. Several laws have been enacted at the state and federal level, as well as in foreign countries, to protect both parties involved in a digital signature transaction. One such law, The Electronic Signatures in Global and National Commerce Act of 2000, renders digital signatures legally binding as long as the consumer or corporate purchaser has affirmatively consented to such use and has not withdrawn such consent. The E-Signature Act does not require “any person to agree to use or accept electronic records or e-signatures.” Moreover, businesses are required to inform consumers and trading partners of the following:

- Their right to withdraw consent to accept electronic transactions
- Procedures for withdrawal of consent
- Whether the consent is for a one-time transaction or ongoing
- How to obtain a paper copy of an electronic record
- The hardware and software requirements for access to and retention of electronic records.

The E-Signature Act also requires that the information remain available to all parties that are entitled to access for the period of time required by law, and “in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing or otherwise.” Thirty-seven states have enacted Uniform Electronic Transactions Acts that relate to the federal law, and another eight have legislation in process. Many of the state laws are more specific than the federal laws, so it is important that businesses considering a digital signature-based infrastructure study state, federal, and international laws. This is an emerging area of law, and those that do not stay current could make unwitting, serious errors.

**Digital Accounting Business Risk**

The third area of concern is managing the new business risks introduced by digital signature usage. Digital signature technology causes a pervasive and fundamental change to business processes. As a result, both the accounting and internal audit functions must take on new tasks to protect businesses from new risks. The following are areas where existing accounting practices and expertise may have to be altered to maintain internal control:

- Regularly review all systems utilizing digital procedures, to eliminate costly duplicate manual processing.
- Conduct a quarterly review of CAs to ensure there have been no changes in policy and business practice.
- Legal counsel should review digital practices for compliance with new regulations and legislation at least once a year.
- CA and business partner agreements should be kept current and reviewed for compliance with current laws.
- Private keys, passwords, and other security information should be reviewed and updated at least quarterly.
- Monitor expenditures on digital training and processes quarterly to ensure adequate resources.
- Update storage procedures of digital files on a monthly or more frequent basis, including a test of off-site backup facilities.
- Conduct a quarterly update of digital authorizations, to avoid leaving inappropriate levels of control in place when not needed.

SAS 94 expands the accountant’s responsibility to develop a strong internal control system. Developing good risk-management habits for digital signatures is an essential part of this requirement. Companies that take precautions to make sure that their digital signature program follows sound risk-management guidelines can improve their customer satisfaction and relationships with business partners. By capitalizing on the successful use of digital signatures, businesses can appeal to customers attuned to the changing economy.

**Preparing for Success**

There are many examples of failed digital signature implementations. Some of this can be blamed on the newness of the technology, but digital signatures mostly experience the same troubles that any systems project does. Some common reasons for failed digital signature implementation include: insufficient planning and preparation; underestimated scope of the implementation requirements; infrastructure and procedural costs; unexpected operational and technical incompatibilities with existing systems; and unclear analysis of the expected cost-benefits.

Large corporations and governments have so far been responsible for pushing digital signatures in order to reduce the cost of their paper processing and filing. Despite the advantages, U.S. companies are not adopting the technology as quickly as those in Asia and Europe. At the current level of adoption, companies can still obtain significant strategic advantages with a relatively fast implementation of digital signatures. Whether companies move to adopt the technology now, or wait and are forced by customers and suppliers to adopt it later, digital signatures will soon be a reality for every accounting department.

---

Fritz Grupe, EdD, is professor and chair of the department of accounting and information systems, Stephen G. Kerr, PhD, is an assistant professor of accounting, William Kuechler, PhD, is an assistant professor of information systems, and Nilesh Patel is a graduate student, all at the department of accounting and information systems, the University of Nevada, Reno.