

USPTO PATENT FULL-TEXT AND IMAGE DATABASE

( 1 of 728 )

United States Patent  
Wheeler , et al.

6,425,083  
July 23, 2002

Account authority digital signature (AADS) system

**Abstract**

In a system for performing an action regarding an account in response to an electronic communication received from a sender by a receiver, wherein the electronic communication includes sender identity information associated with the account and a digital signature derived from an electronic message using a private key of a public-private key pair, and wherein the public key of the pair has been associated with the account by the receiver such that the public key is retrievable based on the sender identity information, a method of validating the identity of the sender for the electronic communication includes: (a) retrieving the public key based on the received sender identity information; and (b) comparing a function of the public key and the digital signature with a function of the electronic message. Neither a PIN nor a password is required to be transmitted to the receiver for validating the identity of the sender.

Inventors: **Wheeler; Anne McAfee** (Morgan Hill, CA); **Wheeler; Lynn Henry** (Morgan Hill, CA)

Assignee: **First Data Corporation** (Greenwood Village, CO)

Appl. No.: **189159**

Filed: **November 9, 1998**

**Current U.S. Class:**

**713/185**

**Intern'l Class:**

H04K 001/00; H04L 009/00

**Field of Search:**

713/182 380/2

**References Cited** [\[Referenced By\]](#)

U.S. Patent Documents		
<a href="#">3962539</a>	Jun., 1976	Ehram et al.
<a href="#">4200770</a>	Apr., 1980	Hellman et al.
<a href="#">4218582</a>	Aug., 1980	Hellman et al.
<a href="#">4405829</a>	Sep., 1983	Rivest et al.
<a href="#">4408203</a>	Oct., 1983	Campbell.
<a href="#">4424414</a>	Jan., 1984	Hellman et al.
<a href="#">4748668</a>	May., 1988	Shamir et al.

# REPORT DOCUMENTATION PAGE

Form Approved  
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

<b>1. AGENCY USE ONLY (Leave blank)</b>	<b>2. REPORT DATE</b> 11/9/1998	<b>3. REPORT TYPE AND DATES COVERED</b> Patent 11/9/1998	
<b>4. TITLE AND SUBTITLE</b> Account Authority Digital Signature (AADS) System		<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Wheeler, Anne McAfee; Wheeler, Lynn Henry			
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> United States Patent and Trademark Office		<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> IATAC 3190 Fairview Park Drive Falls Church, VA 22042		<b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b>			
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; Distribution unlimited		<b>12b. DISTRIBUTION CODE</b>  A	
<b>13. ABSTRACT (Maximum 200 Words)</b>  In a system for performing an action regarding an account in response to an electronic communication received from a sender by a receiver, wherein the electronic communication includes sender identity information associated with the account and a digital signature derived from an electronic message using a private key of a public-private key pair, and wherein the public key of the pair has been associated with the account by the receiver such that the public key is retrievable based on the sender identity information, a method of validating the identity of the sender for the electronic communication includes: (a) retrieving the public key based on the received sender identity			
<b>14. SUBJECT TERMS</b> IATAC Collection, digital certification		<b>15. NUMBER OF PAGES</b>  18	
		<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> UNCLASSIFIED	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> UNCLASSIFIED	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> UNCLASSIFIED	<b>20. LIMITATION OF ABSTRACT</b> UNLIMITED

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)  
Prescribed by ANSI Std. Z39-18  
298-102

<a href="#">4797920</a>	Jan., 1989	Stein.	
<a href="#">4823388</a>	Apr., 1989	Mizutani et al.	
<a href="#">4825050</a>	Apr., 1989	Griffith et al.	
<a href="#">4850017</a>	Jul., 1989	Matyas, Jr. et al.	
<a href="#">4868877</a>	Sep., 1989	Fischer.	
<a href="#">4885788</a>	Dec., 1989	Takaragi et al.	
<a href="#">5018196</a>	May., 1991	Takaragi et al.	
<a href="#">5097504</a>	Mar., 1992	Camion et al.	380/23.
<a href="#">5140634</a>	Aug., 1992	Guillou et al.	
<a href="#">5214703</a>	May., 1993	Massey.	
<a href="#">5225978</a>	Jul., 1993	Petersen et al.	
<a href="#">5231668</a>	Jul., 1993	Kravitz.	
<a href="#">5453601</a>	Sep., 1995	Rosen.	
<a href="#">5502766</a>	Mar., 1996	Boebert et al.	380/25.
<a href="#">5509071</a>	Apr., 1996	Petrie, Jr. et al.	
<a href="#">5534855</a>	Jul., 1996	Shockley et al.	
<a href="#">5539828</a>	Jul., 1996	Davis	380/50.
<a href="#">5563946</a>	Oct., 1996	Cooper et al.	380/4.
<a href="#">5590197</a>	Dec., 1996	Chen et al.	
<a href="#">5604801</a>	Feb., 1997	Donlan et al.	
<a href="#">5606609</a>	Feb., 1997	Houser et al.	
<a href="#">5615266</a>	Mar., 1997	Altschuler et al.	
<a href="#">5619574</a>	Apr., 1997	Johnson et al.	
<a href="#">5623637</a>	Apr., 1997	Jones et al.	
<a href="#">5625690</a>	Apr., 1997	Michel et al.	
<a href="#">5636280</a>	Jun., 1997	Kelly.	
<a href="#">5659616</a>	Aug., 1997	Sudia.	
<a href="#">5671279</a>	Sep., 1997	Elgamal.	
<a href="#">5671285</a>	Sep., 1997	Newman.	
<a href="#">5677953</a>	Oct., 1997	Dolphin	380/4.
<a href="#">5694471</a>	Dec., 1997	Chen et al.	
<a href="#">5708780</a>	Jan., 1998	Levergood et al.	
<a href="#">5715314</a>	Feb., 1998	Payne et al.	
<a href="#">5721779</a>	Feb., 1998	Funk.	
<a href="#">4734564</a>	Mar., 1998	Boston et al.	
<a href="#">5724424</a>	Mar., 1998	Gifford.	
<a href="#">5751813</a>	May., 1998	Dorenbos.	
<a href="#">5781723</a>	Jul., 1998	Yee et al.	
<a href="#">5796840</a>	Aug., 1998	Davis	380/50.
<a href="#">5812666</a>	Sep., 1998	Baker et al.	
<a href="#">5848161</a>	Dec., 1998	Luneau et al.	

<a href="#">5862324</a>	Jan., 1999	Swang et al.	
<a href="#">5878142</a>	Mar., 1999	Caputo et al.	
<a href="#">5887131</a>	Mar., 1999	Angelo.	
<a href="#">5903882</a>	May., 1999	Asay et al.	
<a href="#">5910988</a>	Jun., 1999	Ballard.	
<a href="#">5910989</a>	Jun., 1999	Naccache.	
<a href="#">5943423</a>	Aug., 1999	Muftic.	
<a href="#">5949881</a>	Sep., 1999	Davis	380/25.
<a href="#">5956404</a>	Sep., 1999	Schneier.	
<a href="#">5970147</a>	Oct., 1999	Davis	380/25.
<a href="#">6023509</a>	Feb., 2000	Herbert et al.	380/25.
<a href="#">6044154</a>	Mar., 2000	Kelly.	
<a href="#">6047051</a>	Apr., 2000	Ginzboorg et al.	
<a href="#">6084969</a>	Jul., 2000	Wright et al.	
<a href="#">6092202</a>	Jul., 2000	Veil et al.	
<a href="#">6105012</a>	Aug., 2000	Chang.	
<a href="#">6108644</a>	Aug., 2000	Goldschlag et al.	
<a href="#">6111956</a>	Aug., 2000	Field et al.	
<a href="#">6134325</a>	Oct., 2000	Vanstone et al.	
<a href="#">6161180</a>	Dec., 2000	Matyas et al.	
<a href="#">6161181</a>	Dec., 2000	Haynes, III et al.	
<a href="#">6167518</a>	Dec., 2000	Padgett et al.	
<a href="#">6192130</a>	Feb., 2001	Otway.	
<a href="#">6199052</a>	Mar., 2001	Mitty et al.	
<a href="#">6202151</a>	Mar., 2001	Musgrave et al.	
<a href="#">6230269</a>	May., 2001	Spies et al.	
<a href="#">6263447</a>	Jul., 2001	French.	
<a href="#">2001/0000053</a>	Mar., 2001	Lapsley et al.	
<b>Foreign Patent Documents</b>			
2271178	May., 1999	CA.	

### Other References

- Burton S. Kaliski, Jr., Some Examples of the PKCS Standards, An RSA Laboratories Technical Note, Nov. 1, 1993, RSA Laboratories, Redwood City, CA, pp. 1-15.
- Burton S. Kaliski, Jr., A Layman's Guide to a Subset of ASN.1, BER, and DER, An RSA Laboratories Technical Note, Nov. 1, 1993, RSA Laboratories, Redwood City, CA, pp. 1-36.
- PKCS Editor, PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, Draft 2, Jan. 5, 2001, RSA Laboratories Bedford, MA, pp. 1-60.
- PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Nov. 1, 1993, RSA Laboratories, Redwood City, CA, pp. 1-8.
- PKCS #6: Extended-Certificate Syntax Standard, An RSA Laboratories Technical Note, Nov. 1, 1993, Version 1.5, RSA Laboratories, Redwood City, CA, pp. 1-11.

PKCS #8: Private-Key Information Syntax Standard, An RSA Laboratories Technical Note, Nov. 1, 1993, Version 1.2, RSA Laboratories, Redwood City, CA, pp. 1-5.

Michael J. Wiener, Performance Comparison of Public-Key Cryptosystems, The Technical Newsletter of RSA Laboratories, a division of RSA Data Security, Inc., Summer 1998, vol. 4, No. 1, RSA Laboratories, San Mateo, CA, pp. 1-23.

George Apostolopoulos, et al., Securing Electronic Commerce: Reducing the SSL Overhead, IEEE Network, Jul./Aug. 2000, vol. 14, Issue 4, pp. 1-16.

Ueli Maurer, Modelling a Public-Key Infrastructure, Sep. 1996, Proc. 1996 European Symposium on Research in Computer Security, Lecture Notes in Computer Science, Berlin: Springer-Verlag, Rome, Italy, Department of Computer Science, Swiss Federal Institute of Technology, Zurich, Switzerland, pp. 1-26.

Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-1, Jan. 11, 1994, pp. 1-45, CSL Bulletin For FIPS 140-1 pp. 1-6, Validated FIPS 140-1 Cryptographic Modules 2001, 2000, 1999, 1998, 1997-95, pp. 1-14.

Mark Heroux, A Private Key Storage Server for DCE--Functional Specification, Open Software Foundation Request for Comments: 94.1, allegedly dated Nov. 1996, (web site at <http://www.opengroup.org/rfc/mirror-rfc/rfc94.1.txt>), date of capture Jun. 13, 2001, pp. 1-73.

Peter Cox, Bench-Marking SmartGate, Establishing the Scaleability of V-ONE's SmartGate Security System, Internet SmartWare, Ltd., Jul. 24, 1997, pp. 1-7.

Answers to Frequently Asked Questions about Today's Cryptography, RSA Data Security, Inc., Oct. 5, 1993, Revision 2.0, pp. 1-44.

Announcing the Standard for Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186, May 19, 1994, pp. 1-18.

Sharon Boeyen, Certificate Policies and Certification Practice Statements, Entrust Technologies White Paper, Feb. 1997, Version 1.0, pp. 1-7.

Public-Key Infrastructure (PKI)--The VeriSign Difference, Feb. 3, 2001, Copyright 1999, VeriSign, Inc., pp. 1-21.

Thierry Moreau, Thirteen Reasons to Say `No` to Public Key Cryptography, Draft paper, Mar. 4, 1998, CONNOTECH Experts-Conseils, Inc., Montreal, Quebec, Canada, pp. 1-5.

"X9 Overview," American Bankers Association web page (web site at <http://www.x9.org/aboutX9.htm>), allegedly dated 1998, date of capture Jan. 11 1999, 3 pp.

"X9.59 Working Draft" American Bankers Association; American National Standard X9.59-199X, For the Financial Services Industry: Account-Based Secure Payment Objects, allegedly dated Sep. 25, 1998, pp. 1-25.

Lynn Wheeler, Account Authority Digital Signature Model web page (web site at <http://www.garlic.com/about.lynn/aadsover.htm>) believed available at website after Nov. 8, 1997, date of capture Oct. 2, 2001, 5 pp.

Burton S. Kaliski Jr., An Overview of the PKCS Standards, An RSA Laboratories Technical Note, Nov. 1, 1993, RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS), pp. 1-27.

Public Key Cryptography, NIST Special Publication 800-2, Apr. 1991, available at <http://csrc.nist.gov/publication/nistpubs/800-2/800-2.txt>, pp. 1-138.

Guideline for Implementing Cryptography in the Federal Government, NIST Special Publication 800-21, Nov. 1999, pp. 1-138.

Guideline for the Use of Advanced Authentication Technology Alternatives, FIPS Publication 190, Sep. 28, 1994, available at <http://csrc.nist.gov/publications/fips/fips190/fip190.txt>, pp. 1-55.

Building A Foundation of Trust in the PC, The Trusted Computing Platform Alliance, allegedly dated Jan. 2000 (web site at <http://www.trustedpc.org>), pp. 1-9.

Trusted Platform Module (TPM) Security Policy (A Part of the "TCPA Security Policy"), Version 0.45, allegedly dated Oct. 2, 2000, pp. 1-13.

Trusted Platform Module Protection Profile (TPMPP) (A Part of the "TCPA Security Policy"), Version 0.45, allegedly dated Sep. 14, 2000, pp. 1-151.

TCPA PC Specific Implementation Specification, Version 0.95, allegedly dated Jul. 4, 2001, pp. 1-70.

Common Criteria for Information Technology Security Evaluation, Smart Card Security User Group, Smart Card Protection Profile, draft Version 2.1d, allegedly dated Mar. 21, 2001, pp. 1-194.

Xp.84-2000, **Biometric** Information Management and Security for the Financial Services Industry, draft version, allegedly dated Dec. 2000, pp. 1-141.

Security Requirements for Cryptographic Modules, FIPS Publication 140-2, May 25, 2001, pp. 1-62.

Secure Hash Standard, FIPS Publication 180-1, Apr. 17, 1995, pp. 1-24.

Digital Signature Standard (DDS), FIPS Publication 186-2, Jan. 27, 2000, pp. 1-72.

Entity Authentication Using Public Key Cryptography, FIPS Publication 196, Feb. 18, 1997, pp. 1-52.

Computer Data Authentication, FIPS Publication 113, May 30, 1985, available at [www.itl.nist.gov/fipspubs/fip113.htm](http://www.itl.nist.gov/fipspubs/fip113.htm), date of capture Jan. 16, 2001, pp. 1-7.

Hettinga's Best of the Month, Journal of Internet Banking and Commerce, allegedly dated Mar. 31, 1999, available at <http://www.arraydev.com/commerce/JIBC/9801-20.htm>, pp. 1-4.

The Electronic Commerce Challenge, Journal of Internet Banking and Commerce, allegedly dated Mar. 31, 1999, available at <http://www.arraydev.com/commerce/JIBC/9811-06.htm>, pp. 1-2.

Sales Brochure for APPROVEIT, electronic approval management software, by SilanisTechnology, Inc., allegedly dated Jul. 18, 2000, pp. 1-12.

Public Key Infrastructure, An NSS Group White Paper, by Bob Walder, undated, available at <http://www.nss.co.uk/WhitePapers/PublicKeyInfrastructure.htm> on Jan. 25, 2001, pp. 1-18.

Smart Card & Security Basics, Cardlogix, Inc. brochure, allegedly dated: Q1-Q2 2000, pp. 3-36.

Understanding Public Key Infrastructure (PKI), Technology White Paper, by RSA Security, Inc., 1999, pp. 1-10.

An Overview of Smart Card Security, Chan, Siu-cheung Charles, allegedly dated Aug. 17, 1997, available at <http://home.hkstar.com/.about.alanchan/papers/smartCardSecurity>, date of capture Jan. 27, 2001, pp. 1-7.

Technical Introduction to CIP 3.0, Taschler, Scott, Sep. 30, 1997, available at <http://www.datakey.com/cardpage/cip.htm>, date of capture Jan. 25, 2001, pp. 1-6.

Smart Cards: Enabling Smart Commerce in the Digital Age, CREC/KPMG White Paper (Draft), May 1998, pp. 1-22.

Silanis, The Bottom Line of e-Business, ApproveIt, Electronic Approval Management Software, marketing brochure.

WhatIs.com, "Pretty Good Privacy," web pages describing PGP software and uses.

"How PGP Works," web pages from [www.pgpi.org](http://www.pgpi.org), containing basic information.

"PGP Certificate Server, Total Network Security," Network Associates, 3965 Freedom Circle, Santa Clara, CA 95054-1203.

"PGP Desktop Security 7.0," PGP Security, 3965 Freedom Circle, Santa Clara, CA 95054-1203.

"Policy Management Agent for SMTP," Network Associates, 3965 Freedom Circle, Santa Clara, CA 95054-1203.

"Inside PGP Key Reconstruction: Technical Details," Revision by Will Price, dated Jul. 25, 2000, A PGP Security, Inc. White Paper.

Article, David C. Stewart, "Account Authority Digital Signatures: Enabling Secure Internet Transactions via Existing Payment Processes & Infrastructure". Date unknown but believed to be subsequent to Apr. 1998. Copy found at <http://www.garlic.com/.about.lynn/aadswp.htm>. The article is provided for its discussion of other methods of digital signatures used in financial transactions.

Article, Stephanie Denny, "The Electronic Commerce Challenge". Date unknown but believed to be Dec. 14, 1998. Copy available at <http://www.arraydev.com/commerce/JIBC/9811-06.htm>. This article is provided for its discussion of the Secure Electronic Transactions (SET) protocol (1995).

Mailing list article, Lynn Wheeler, "x9.59 electronic payments and account-authority digital signatures", Jan. 5, 1998. Copy found at Hettinga's Best of the Month, <http://www.arraydev.com/commerce/JIBC/9801-20.htm>. The article is not believed to be prior art but is provided for its discussion of prior digital signature models and comparison with the present invention.

*Primary Examiner:* Decady; Albert  
*Assistant Examiner:* Zand; Kambiz  
*Attorney, Agent or Firm:* Morris, Manning & Martin, LLP

---

### *Claims*

---

What is claimed is:

1. In a system for performing an action regarding an account in response to an electronic communication received from a sender by a receiver, wherein the electronic communication includes sender identity information associated with the account and a digital signature derived from an electronic message using a private key of a public-private key pair, and wherein the public key of the pair has been associated with the account by the receiver such that the public key is retrievable based on the sender identity information, validating the identity of the sender for the electronic communication only by performing a method consisting of the steps of:

- (a) retrieving the public key based on the sender identity information received in the electronic communication; and
- (b) comparing a function of the public key and the digital signature with a function of the electronic message,

whereby a comparison resulting in a match validates the identity of the sender.

2. In a system for performing an action regarding an account in response to an electronic communication received from a sender by a receiver, wherein the electronic communication includes sender identity information associated with the account and a digital signature derived from an electronic message using a private key of a public-private key pair, wherein the public key of the pair has been associated with the account by the receiver such that the public key is retrievable based on the sender identity information, and wherein neither a PIN nor a password is required to be transmitted to the receiver for validating the identity of the sender, a method of validating the identity of the sender for the electronic communication comprising the steps of:

- (a) retrieving the public key based on the sender identity information received in the electronic communication; and
- (b) comparing a function of the public key and the digital signature with a function of the electronic message,

whereby a comparison resulting in a match validates the identity of the sender.

3. In a system for performing an action regarding an account in response to an electronic communication received from a sender by a receiver, wherein the electronic communication includes sender identity information for the account comprising other than an account number and a digital signature derived from an electronic message using a private key of a public-private key pair, and wherein the public key of the pair has been associated with the sender identity information by the receiver such that the public key is retrievable based on the sender identity information, a method for validating the identity of the sender for the electronic communication comprising the steps of:

- (a) retrieving the public key based on the sender identity information received in the electronic communication; and
- (b) comparing a function of the public key and the digital signature with a function of the electronic message,

whereby a comparison resulting in a match validates the identity of the sender.

4. In a system for performing an action regarding an account in response to an electronic communication received from a sender by a receiver, wherein the electronic communication is the only electronic communication received from the sender by the receiver relating to the action, wherein the electronic communication includes sender identity information associated with the account and a digital signature derived from an electronic message using a private key of a public-private key pair, and wherein the public key of the pair has been associated with the sender identity information by the receiver such that the public key is retrievable based on the sender identity information, a method for validating the identity of the sender for the electronic message comprising the steps of:

- (a) retrieving the public key based on the sender identity information received in the electronic communication; and
- (b) comparing a function of the public key and the digital signature with a function of the electronic message,

whereby a comparison resulting in a match validates the identity of the sender.

5. The system of claims 1, 2, 3, or 4, wherein the public key is associated with the account in a computer database.

6. The system of claims 1, 2, 3, or 4, wherein the electronic communication includes the electronic message.

7. The system of claims 1, 2, 3, or 4, wherein the electronic message is implied from the receipt of the electronic communication.

8. The system of claims 1, 2, 3, or 4, wherein the function of the public key and the digital signature comprises decrypting the digital signature using the public key.

9. The system of claims 1, 2, 3, or 4, wherein the function of the electronic message comprises calculating a hash value of the electronic message.

10. The system of claims 1, 2, 3, or 4, wherein the digital signature is derived within a smart card of the sender.

11. The system of claims 1, 2, 3, or 4, wherein the digital signature is received from the sender within a terminal of a third-party and then forwarded to the receiver.

12. The system of claims 1, 2, 3, or 4, wherein the electronic communication is received over a secure network.

13. The system of claims 1, 2, 3, or 4, wherein the electronic communication is received over an insecure network.

14. The system of claim 13, wherein the network comprises the Internet.

15. The system of claims 1, 2, 3, or 4, wherein the electronic communication is received encrypted.

16. The system of claims 1, 2, 3, or 4, wherein the electronic communication is received unencrypted.

17. The system of claims 1, 2, 3, or 4, wherein the receiver is a financial institution and the action on the account comprises a financial transaction.

18. The system of claims 1, 2, 3, or 4, wherein the electronic communication includes the public key.

19. The method of claims 1, 2, 3, or 4, wherein the sender identity information comprises the account number.

20. The method of claims 1, 2, 3, or 4, wherein the sender identity information comprises other than the account number.



21. The system of claims 1, 2, 3, or 4, wherein the public key was associated with the account when the account was first established.
22. The method of claim 19, wherein the public key was provided by the sender to the receiver.
23. The method of claim 19, wherein the public key was provided to the sender by the receiver.

---

### *Description*

---

#### FIELD OF THE INVENTION

The field of the invention relates to digital signatures, and particularly, using digital signatures to reliably identify a sender and the accuracy of an electronic message without using certification authorities.

#### BACKGROUND OF THE INVENTION

The increase in electronic commerce has increased the focus on security of the electronic transactions using this medium of commerce. In the world of computer transactions and electronic contracts, there is no face-to-face acknowledgement to identify the consumer or other person wishing to perform the transaction. As institutions become more reliant on computers, they have modified their business infrastructure (i.e., their "business process") in an attempt to keep up with electronic commerce. The business process of an institution includes the methods used to interact with a customer (e.g., how transactions occur, what information is required from the customer, help desks to support the customer), the information contained in customer accounts, the databases used and how they are modified by the institution, and personnel training.

Institutions and persons desiring to utilize electronic commerce are faced with several issues regarding electronic transactions. The first issue is whether the person requesting the transaction is who they say they are ("identification"). And the second issue is whether the requested transaction is actually the transaction intended to be requested ("accuracy"). In other words, whether the requested transaction has been compromised, either fraudulently or through transmission errors, during the course of transmitting and receiving the request.

To address the identity of the person requesting the transaction, current financial business processes bind information in accounts to authenticate non-face-to-face transactions. For example, an account holder's mother's maiden name, a personal identification number (PIN), and a social security number have all been used and integrated into the current financial infrastructure to aid in reliably identifying someone requesting a non-face-to-face transaction.

To address the accuracy of the electronic message being sent and the identity of the person sending the electronic message, digital signatures are utilized. Digital signatures are used with electronic messages and provide a way for the sender of the message to electronically "sign" the message as a way of providing proof of the identity of the sender and the accuracy of the message. In a digital signature system, a sender digitally "signs" the message using a private key (encryption software used to create a digital signature). The receiver validates the sender's digital signature by using the sender's public key (software used to decrypt the digital signature) sent to the receiver by the sender.

While, digital signatures provide some assurance accuracy to the message and the identity of the sender, they are also subject to security risks. These risks include compromised private and public keys or merchant fraud. To address the security risks and validate the digital signatures, computer technology has developed "certification authorities" to be used in a Certificate Authority Digital Signature system (CADS). In a CADS system, certification authorities are third parties that essentially "vouch" for the validity of a digital signature's public key and, hence, the validity of the digital

signature.

However, certification authorities used in the CADS system come with the inherent risk, such a expired certification authority and compromised private keys which affect the entire public key infrastructure. In addition, the increased reliability provided by certification authorities do not easily combine with the business process currently established.

Therefore, there is a need in the art is a method to increase the reliability of electronic transactions while not imposing significant modifications on the business processes already in place.

## SUMMARY OF THE INVENTION

The present invention meets the needs described above by providing a method of reliably identifying the sender of an electronic message and determining the accuracy of an electronic message while utilizing the current standard business processes.

The current financial infrastructure can extend existing business processes to support high integrity electronic commerce by implementing the present invention. One embodiment of the present invention can be implemented as the Account Authority Digital Signature (AADS) system. The AADS system uses digital signatures along with validation procedures that can be implemented within current institutional business processes to identify a sender of an electronic message and determine the accuracy of the electronic message being sent.

The present invention simplifies its implementation by leveraging existing account infrastructures and by operating within existing business processes. In addition, the present invention utilizes electronic signatures in the business process for increased reliability. Yet, however, the present invention does not rely on third parties (i.e., certification authorities) for authorization, thereby avoiding any security risks or other systemic risks associated with the third parties. And finally, no new databases need to be developed to implement the present invention. Generally described, the identity of a sender of an electronic message is validated by using sender validation information along with other sender identity information stored at an institution's or person's computer system and applying the sender validation information to the encoding information received by the computer system. The sender validation information may be the sender's public key in a digital signature system.

The present invention utilizes the accuracy of electronic encoding, e.g., digital signatures, and provides a method to incorporate them into the current business processes. An institution records an encoding key and associates it with account information from the sender. This initial recording may be performed using any of the validation procedures utilized today by a business institution, for example, when the sender is opening an account and must show proof of identity.

After the initial validation of the encoding key, validating future electronic transactions occur by including encoding information that can be deciphered using the valid encoding key initially stored. To validate an electronic transaction, the sender sends the electronic transaction message, the encoding information and sender identity information to the person or institution from which the sender desires validation. Having received this information, the computer system automatically retrieves the encoding information stored in the computer system that is associated with the sender identity information. The computer system then validates the electronic transaction message by applying the retrieved encoding key to the encoding information and analyzes the electronic transaction message to validate the identity of the sender and the accuracy of the message.

This validation may be performed in a digital signature system by applying a hashing algorithm to the electronic message and comparing the results to the results of applying the public key to the digital signature received.

The encoding information may be entered into a terminal via of a smart card or via another computer system. The encoding information, electronic message and sender identity information may be sent to the computer system

performing the validation via a closed network or via an open network, such as the Internet.

These and other advantages of the present invention may be more clearly understood and appreciated from a review of the following detailed description of the disclosed embodiments and by reference to the appended drawings and claims.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram depicting an exemplary debit card system as it exists in the prior art.

FIG. 2 is a block diagram depicting the Certification Authority Digital Signature (CADS) system as it exists in the prior art.

FIG. 3 is a block diagram depicting the digital signature process.

FIG. 4 is a block diagram depicting the effect of a security breach in the existing debit card system.

FIG. 5 is a block diagram depicting the effect of a security breach in the existing CADS system.

FIG. 6 is a block diagram of an exemplary computing environment in an embodiment of the present invention.

FIG. 7 is a block diagram of the components of an embodiment of the present invention.

FIG. 8 is a block diagram depicting an embodiment of the present invention as it is implemented using a financial institution, a merchant and a customer.

FIG. 9 is a flowchart depicting the steps performed in implementing an embodiment of the present invention.

## DETAILED DESCRIPTION

The present invention provides a method for reliably identifying the sender of an electronic method and determining the accuracy of an electronic message while utilizing current standard business processes.

Electronic commerce is currently used and implemented in several existing systems. The conventional debit card system is one example. The debit card system attempts to identify the sender of the electronic message (e.g., the message of "Withdraw \$200 from my account") while working in the current business processes. In other words, it utilizes a PIN as merely another validation mechanism. However, the debit card system does not verify the accuracy of the message. In addition, because of the security risks, the debit card system is not utilized on an open network, such as the Internet, thereby limiting its access to electronic commerce.

The Certification Authority Digital Signature (CADS) system is another example of a system used to implement electronic commerce. The CADS system provides message accuracy and may be used in open networks, such as the Internet. However, CADS also has inherent systemic risks and requires reliance on third parties to "authorize" the digital signature of the sender of the electronic message. In addition, the CADS system is difficult to implement using standard business processes utilized today.

Both the debit card system and the CADS system can have severe consequences in the event the security of either system is compromised. The debit card and CADS systems, as well as the security risks associated with each, are discussed further in FIGS. 1-2 and 3-4.

Turning now to the figures, FIG. 1 is a block diagram depicting a conventional debit card system as it exists in the

prior art. Typically, a customer enters account information and a personal identification number (PIN) into a terminal 100. The account information is generally stored on magnetic tape attached to a card that is given to the customer so that the customer may enter it into the terminal 100. Upon entering the account information and the PIN, the terminal then formats this data and sends it across a closed network 105 to the main computer 110 that validates the PIN with an associated account that has been entered by the customer. The PIN was stored in a field along with other account information in the main computer previously. The PIN is typically associated with the customer when the account is established but generally not through the network 105. Normal procedures provide for the customer to validate their identity when the account is opened or prior to associating a PIN to the customer's account. This would verify to the institution that the person establishing the account is who they claim to be and increases the reliability that when the PIN is used, the customer assigned the PIN is the one using it.

Upon validating the PIN with the associated account, the main computer 110 then accepts or rejects the PIN and sends the results back through the network 105. The terminal, having received the acceptance or rejection, then either continues to process the customer's transaction or denies customer access to the account.

The PIN used in the debit card system is the same for all transactions. In other words, no matter what transaction the customer wishes to initiate with the main computer, i.e., regardless what message is sent to the main computer by way of the terminal, the PIN stays exactly the same.

The terminal 100 used in the debit card system is a basic terminal that is used to format the entered information to send to the main computer 110. In addition, the terminal 100 may perform some function such as dispensing cash or other functions specific to the account. However, the terminal 100 is generally a dumb terminal only used to facilitate the customer's interaction with the main computer 110 (i.e., the terminal is not typically used for purposes other than to interact with financial institutions). The terminal 100 communicates with the main computer 110 by network 105.

The network 105 used in the debit card system is typically a closed network that is set up specifically for use between the terminal 10 and main computer 110. While it is possible that others may break into the network, generally, the network 105 is not used for other traffic other than messages sent between the terminal 100 and main computer 110.

The main computer 110 used in the debit card system is generally housed at the institution containing the account and contains all the records for the institution relative to the account and the PIN. When the account is initially set up, all information required to process this transaction as well as potentially other transactions within the institution is validated. For security reasons, the required information was validated in either face-to-face or in some other manner that can validate the customer's identity. Consequently, there is a direct validation of the account to the customer when the account is established. As stated earlier, the business processes set up in many financial institutions today follow this model. These processes include manuals, computer databases and records, held desks and personnel training.

FIG. 2 is a block diagram depicting the known Certification Authority Digital Signature (CADS) system as it exists in the prior art. The CADS system relies on the digital signatures and traditional public key infrastructure regarding issuing certificates that are signed by a certification authority. (see FIG. 3 regarding a description of digital signatures and their usage). A certification authority attests to the validity of the public key and sometimes, depending on the authority, checks the validity of the private key and the identity information of the entity that the certificate is issued to. The sender then sends the certificate, which is a digital signature incorporating the sender's digital signature, issued by the certification authority, the message, and the sender's public key to the receiving party. The intent is that the receiving party will trust the certification authority's verification and also will be able to validate the certification authority's digital signature and the sender's message using the contents of the information sent by the sender and a public key of the certification authority.

In FIG. 2, the sender 201 creates a digital signature using the sender's message 225. (Additional discussion on creation of a digital signature is provided below in relation to FIG. 3.) Prior to sending the message to the receiver 242, it is preferable to validate the sender's message and therefore the sender submits it to a certification authority. The intent of

the certification authority is to confirm that the identified sender is sending the message. Continuing with FIG. 2, the sender then has the digital signature "authorized" by a Certification Authority 1 (CA1) 205. The CA1 has, in advance, identified the public key associated with the sender. Therefore, the CA1205 checks the current digital signature with the sender to ensure that it is the same as what was established previously.

An example of a certification authority includes certifying the identity of specific banks. However, as there are no rules or laws regarding who is a certification authority and who is not, in some instances, the receiver may not "trust" the certification authority. The receiver might be a large scale institution that does not trust a certification authority that deals with just a few customers or small institutions. Specifically, the receiver may not trust that the security is as high as it expects from the certification authority. Therefore, the receiver would require a higher level certification authority. In cases like this, the first certification authority also needs to be authorized. This is depicted in FIG. 2 by CA1 sending its digital signature to certification authority 2 (CA2) 210. CA2 is, in essence, an authority that confirms the identity of other first "level" certification authorities. In the example provided, CA2 may confirm the identity of a financial institution versus just a bank as in CA1.

This additional certification authority may still not rise to the level of security required by the receiver so yet another certification authority may be necessary. This is depicted by CA2210 creating a digital signature using CA1's 205 digital signature and sending CA2's digital signature on to CA3215. CA3215 could be just another higher level certification authority that checks all institutions. And as is apparent, this hierarchy of certification authorities could continue ad infinitum. However, at some point, the sender and receiver are satisfied with the level of certification authorities and, in FIG. 2, ends with CA3215. CA3's digital signature is created and used by the sender. The sender 201 then attaches CA3's digital signature 235 to the sender's message 225 along with the sender's public key 230 into a complete message block depicted by 220. The space required for the digital signature may be significant in relation to the message. Generally, the classic electronic transaction message comprises 80 bytes and the sender's digital signature comprises 60 bytes. However, for each certification, it requires another 2,000 bytes. The size of the message the sender is sending over the network 240 is increased substantially by using certification authorities. The sender then having combined the message, the public key and CA3's digital signature, sends this complete packet over the network 240 to the receiver 242.

The receiver now has to validate the sender's message to ensure that the authentic sender is sending the message and not a third party using the sender's identity. Having received the complete packet 220, the receiver 242 then begins applying public keys to the digital signatures received in the packet. Typically, the receiver will already have the public key of the final certification authority used by the sender. In cases where it is not clear, the sender must also send the public key to the receiver of the final certification authority.

In the instance shown in FIG. 2, because CA3 was the final certification authority, the receiver then applies CA3's public key to CA3's digital signature 235 that was received in the packet 220. Applying CA3's public key to the CA3's digital signature creates CA2's digital signature in addition to providing CA2's public key (not shown). Now having CA2's digital signature 245 and CA2's public key, the receiver applies CA2's public key to CA2's digital signature 250 to create CA1's digital signature 250 and CA1's public key (not shown). The receiver then must apply CA1's public key to CA1's digital signature to create the initial sender's digital signature 255.

While it is shown that this process is performed three times because there have been three certification authorities, it will be recognized that this process would occur as many times as there are certification authorities used for the sender's message. It is clear that this process also adds significant overhead processing to the validation of the sender's identity. Particularly with the more certification authorities used, the processing and resources required purely for the task of validating the sender is increased dramatically.

Finally arriving at the sender's digital signature 255, the receiver then validates the message. The receiver does this by using the sender's message 225, the sender's public key 230 that had been sent in the initial packet 220, as well as the sender's digital signature 255 that was created from this process of certification authority validation just described. The

receiver uses all these components to then validate the sender's digital signature 240. The receiver may send back the results of the validation, or if the validation was successful, act on the message sent.

While the conventional CADS system depicted in FIG. 2 provides some degree of reliability confirming the sender's identity, standard business processes are not equipped to deal with these kind of certification authority validation procedures.

FIG. 3 depicts how a message is validated using the digital signature process. Initially, the sender creates a message 300 and applies a hashing algorithm to the message 300 to create a modified message 305. Because of the hashing algorithm, the modified message typically is a much smaller version of the actual message itself.

The modified message 305 that is created using the hashing algorithm and the sender's message 300 is not only smaller, but is also unique to the message. In other words, as the message changes, the modified message will also change after applying the hashing algorithm. The modified message is then encrypted with the sender's private key.

The process of using a digital signature generally requires a private and a public key. These keys are typically obtained from software houses and developers that create encryption programs. The private key is used by the sender and only by the sender. To maintain the security, as the name implies, the private key is intended to be kept private to the sender and not for public dissemination. This is the only time in the process, i.e., applying the private key to the modified message 305 to create the digital signature 310, where the private key is used.

The creation of the sender's digital signature described above in FIG. 3 can be performed at the sender's local computer, or in some cases, on a smart card. The use of smart cards are well know to those skilled in the art. The end result of the sender's process is that the sender has created a digital signature. And as stated, this digital signature is message specific, i.e., if any letter or any component of the message was changed, this digital signature would also change. The digital signature is also specific to the individual sender, i.e., the private key encryption method is only for that sender.

The sender then sends the sender's message with a public key, if the receiver does not already have one, and the digital signature to a receiver (this "sending" process is not shown). The receiver then takes the sender's message 300 and applies the same hashing algorithm described above for the sender to create the modified message 305. Ideally, this should be the same modified message. The only case where the sender's and receiver's modified message is different is if the message was corrupted either by the sender after having applied the digital signature to it, by transmission errors or someone fraudulently intercepting the message and attempting to change its contents.

Still referring to FIG. 3, next the receiver then takes the sender's digital signature and applies the sender's public key to the digital signature. As implied, the public key is available for public use by the sender without losing any security of the sender's private key. The receiver then applies the public key to create the decrypted digital signature 315. The decrypted digital signature and the modified message 305 are then compared by the receiver. If they both match up and are identical, then the receiver knows that the message was encrypted with a sender's private key and was the same message that has been received. However, because it is not known for sure whether the sender's private key has been corrupted (e.g., stolen), the receiver is still not absolutely sure that the sender identified in the message actually is the one who sent it.

FIG. 4 is a block diagram depicting the effect of a security breach (e.g., someone stealing someone's PIN and account info.) in the existing debit card system. In this case, the fraudulent customer enters account information and a PIN to a terminal 400 and requests a transaction. The same PIN is used for all transactions and the PIN typically is a easily remembered non-complex set of numbers and/or letters that can be entered by the customer. Once the PIN has been corrupted for a one message, that same PIN can be used for other messages that the fraudulent customer wishes to send.

The terminal 400 having received the account information and PIN from the fraudulent customer then, as expected, sends this fraudulent information on to the main computer 410 through the network 405. The main computer 410 is not checking the message against the PIN. It merely receives the PIN and checks it against the account that has been stored already in the main computer 410. If the fraudulent customer has done his job and has stolen the correct PIN, then the transaction will be validated and the acceptance will be passed on and the fraudulent customer will have access to some else's account.

Another area of concern, not depicted in FIG. 4, is when a third party steals the customer's PIN by tapping into the network 405. Since no encoding or encrypting is performed on the PIN, and since the same PIN is used for all messages, once someone who has tapped into the network to obtain this information, they are not required to perform any decryption on the message and can receive the PIN from the network. Once they have access to this PIN, they can then get into the customer's account and send any messages such as checking the account balance and withdrawing funds from an account. Having one PIN for all messages facilitates this type of security breach.

FIG. 5 depicts the effect of a security breach, i.e., the stealing of a certification authority's private key by a third party, in the existing CADS system. When a certification authority's private key is stolen by a third party, all messages certified by that authority is suspect because the third party, not the certification authority, may generate false messages which appear to authorized by the certification authority.

In this case, an authentic sender is not attempting to send a message 500, and in this example, CA1 has not applied any digital signature because there is no message. But what has occurred is that there has been a security breach in the CA2. For example, CA2's private key has been stolen. In general, the effect of having the CA2's private key stolen is that it can then mask as any of the CA1's or senders relying on CA2 for certification even though they are not attempting to send a message. In addition, a corrupted CA2 private key allows the creation of fictitious CA1's or senders that do not exist, yet will appear valid because they are certified by CA2. So, if a certification authority can validate that a specific merchant is requesting a transaction when that merchant is indeed not requesting a transaction, this facilitates the fraudulent use of the electronic commerce system.

Continuing with FIG. 5, a fraudulent message 510 is created using a fraudulent public key and the fraudulent private key compromised from CA2. A digital signature is created using this information and using CA2's compromised private key is sent to CA3 for validation. Because the private key has been compromised, these messages and the digital signature is validated by CA3 and, consequently, the digital signature and fraudulent information is sent on to the receiver 536.

The receiver then receives the fraudulent message 510, the fraudulent public key 515, and the fraudulent digital signature 520 that was created by the compromised CA2. The receiver then runs through the process as described in FIG. 2 to validate the certification authority. The receiver applies CA3's public key, which is valid, and creates CA2's digital signature 540. It then applies CA2's public key to CA2's digital signature and this creates a valid digital signature for CA1545, even though CA1 has not digitally signed this message. The receiver then applies CA1's public key to what appears to be a valid digital signature of CA1. This creates a valid digital signature of the sender 550. This is the case even though the sender has not created a message, nor has CA1 validated it in any manner. The receiver, using the fraudulent message 510 and the fraudulent public key 515, then validates the sender's digital signature that was created using the fraudulent and compromised private key of CA2.

The present invention addresses the security needs identified above by providing a method of reliably identifying the sender of an electronic message and determining the accuracy of an electronic message while utilizing the current standard business processes. Below is a description of various embodiments of the present invention.

#### Exemplary Operating Environment

FIG. 6 and the following discussion are intended to provide a brief, general description of a suitable computing

environment in which the invention may be implemented. While the invention will be described in the general context of an application program that runs on an operating system in conjunction with a personal computer, those skilled in the art will recognize that the invention also may be implemented in combination with other program modules. Generally, program modules include routines, programs, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that the invention may be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

With reference to FIG. 6, an exemplary system for implementing the invention includes a conventional personal computer 20, including a processing unit 21, a system memory 22, and a system bus 23 that couples the system memory to the processing unit 21. The system memory 22 includes read only memory (ROM) 24 and random access memory (RAM) 25. A basic input/output system 26 (BIOS), containing the basic routines that help to transfer information between elements within the personal computer 20, such as during start-up, is stored in ROM 24. The personal computer 20 further includes a hard disk drive 27, a magnetic disk drive 28, e.g., to read from or write to a removable disk 29, and an optical disk drive 30, e.g., for reading a CD-ROM disk 31 or to read from or write to other optical media. The hard disk drive 27, magnetic disk drive 28, and optical disk drive 30 are connected to the system bus 23 by a hard disk drive interface 32, a magnetic disk drive interface 33, and an optical drive interface 34, respectively. The drives and their associated computer-readable media provide nonvolatile storage for the personal computer 20. Although the description of computer-readable media above refers to a hard disk, a removable magnetic disk and a CD-ROM disk, it should be appreciated by those skilled in the art that other types of media which are readable by a computer, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, and the like, may also be used in the exemplary operating environment.

A number of program modules may be stored in the drives and RAM 25, including an operating system 35, one or more application programs 36, the Account Authority Digital Signature (AADS) module 37, and program data 38. A user may enter commands and information into the personal computer 20 through a keyboard 40 and pointing device, such as a mouse 42. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 21 through a serial port interface 46 that is coupled to the system bus, but may be connected by other interfaces, such as a game port or a universal serial bus (USB). A monitor 47 or other type of display device is also connected to the system bus 23 via an interface, such as a video adapter 48. In addition to the monitor, personal computers typically include other peripheral output devices (not shown), such as speakers or printers.

The personal computer 20 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 49. The remote computer 49 may be a server, a router, a peer device or other common network node, and typically includes many or all of the elements described relative to the personal computer 20, although only a memory storage device 50 has been illustrated in FIG. 6. The logical connections depicted in FIG. 6 include a local area network (LAN) 51 and a wide area network (WAN) 52. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

When used in a LAN networking environment, the personal computer 20 is connected to the LAN 51 through a network interface 53. When used in a WAN networking environment, the personal computer 20 typically includes a modem 54 or other means for establishing communications over the WAN 52, such as the Internet. The modem 54, which may be internal or external, is connected to the system bus 23 via the serial port interface 46. In a networked environment, program modules depicted relative to the personal computer 20, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communication's link between the computers may be used.



FIG. 7 is a block diagram of the components of the preferred embodiment of the present invention. This embodiment of the present invention utilizes the paradigm of the digital signatures as described with respect to FIG. 3 and merges it into business processes utilized today.

Prior to sending a message to the receiver, the sender provides the sender's public key 730 to the receiver 720. The receiver then stores the sender's public key 725, which will be used to validate electronic messages that will be sent to the receiver. In one embodiment, the sender provides the public key to the receiver when the sender initially establishes an account with the receiver. It is preferable that the receiver stores the sender's public key along with other sender account information such as name, address, PIN, mother's maiden name, or other security information that is associated with an account. It is also preferable to not send the sender's public key to the receiver in the same electronic message that the sender desires to have validated.

The sender 710 then creates a sender's message 700 and attaches the digital signature 705. The digital signature was created by the process described either in FIG. 3 or by another process as known to those skilled in the art. It will be recognized by those skilled in the art that the digital signature can be any security device used to associate a specific message with a sender.

The sender sends the sender's message 700 and the sender's digital signature 705 to the receiver 720 by way of the network 715. The network 715 can either be a closed network as is used in the debit card system, or it can be an open network such as the Internet. Because the digital signature is applied, if 715 is an open network such as the Internet, there is a low probability that someone monitoring for traffic and trying to "steal" messages and private information will be able to decrypt the digital signature of the sender.

Note that in this embodiment, the sender is not sending the public key with the message, and the sender is also not using any certification authorities to authorize this message. Also note that because the standard business process supports validation criteria, adding another criteria, such as a public key, requires minimal modification to the business process.

The receiver 720 then receives the sender's message 700 and the sender's digital signature 705. The receiver 720 then automatically retrieves the prestored public key associated with the sender's other account information and validates the sender's digital signature using this prestored public key. Because a digital signature is being used, each message is encrypted and no one tapping into the network 715 will be able to modify the message as it proceeds to the receiver. If the message is modified or corrupted in any manner, the message will fail the validation process and the receiver will refuse the request.

FIG. 8 is a block diagram depicting an embodiment of the present invention as it is implemented using a financial institution 825, a merchant 812 and a customer 810. The present invention applies in situations where security and the sender's identification is required. One embodiment is a financial institution that uses standard business processes common in the industry today. In this embodiment, the customer 810 generates requests and provides account information 800, as well as generates a digital signature 805. The customer sends this information through the network 815 to a merchant 812. This information can be used under several situations. For example, if a customer is purchasing groceries at a supermarket and has a smart card that contains his or her private key, or when the customer is using his home computer and is trying to purchase a book or other goods over the Internet from a merchant.

The merchant 812 then receives the customer's request and account information 800 and the customer's digital signature 805. The merchant then seeks to have the financial institution authorize the transaction. In other words, the merchant wants the financial institution to confirm the identity of the customer 810 and confirm that there are enough funds in the account to make this purchase. In order to have the transaction authorized, the merchant sends this information to the network 820 to the financial institution 825 for validation. It will be noted that the merchant has not received the private or public key from the customer. The merchant has received a digital signature from the customer and that digital signature will only be valid for this specific request from the customer. If the request is modified in any

way, the digital signature will become invalid. This is important because of the high incidence of merchant fraud perpetrated by merchants. So, if the merchant cannot modify the customer's request in any way without having the digital signature becoming invalid, this will provide a significant savings for the financial institutions and ultimately the customer as well.

The financial institution 825, having received the customer's request and account information 800, and the customer's digital signature 805, then automatically retrieves the public key 830 that has been previously stored and validates 835 the customer's digital signature using the prestored public key 830. Depending on the purpose for which the present invention is implemented, the institution may then act on the customer's request, such as to authorize a transaction involving the customer's account.

When the financial institution is performing an account authorization, any of the methods known to those skilled in the art may be employed while using the present invention. For example, the financial institution may employ a model using an authorization source and a transaction process. Under this model, when used with a credit card transaction, the authorization source interacts with the merchant to receive the customer account information and the transaction request. The transaction processor may be used to interact with the credit card issuing association to approve the transaction. Methods of account approval are many and are considered within the scope of the present invention when the validation of an electronic message is required.

The financial institution 825 then validates the account with the digital signature and returns the results of the validation through the network 820 to the merchant 812. The merchant then accepts or rejects the request by the customer 810, notifying the customer via the network 815. The networks 820 or 815 can be open networks such as the Internet, closed networks, or one could be an open network while the other is a closed network.

It should be noted that because the digital signature is encrypted, the public key is not being sent (i.e., the public key has been prestored at the institution), and no certification authorities are being used, the concern of fraudulent tapping into the network to retrieve sensitive customer or sender information has been greatly reduced. Further note that the merchant has only been a pass through mechanism to confirm the identity of the customer to the bank and to verify account information.

FIG. 9 is a flow chart depicting the steps performed in implementing an embodiment of the present invention. Method 900 begins at the start step 905 and proceeds to step 910 where public key information is stored in a database along with sender identity information about a sender. This may be performed in a manner well known, for example, when someone opens up a checking account and provides identity information, such as mother's maiden name, social security number or other types of information required by institutions that require a high level of confidence of the sender's identity. The sender identity information may be anything that the institution desires, such as account information, sender's name or any other information the institution wishes to use to associate the sender's public key to the sender.

Proceeding to step 920, the sender encrypts a message using the sender's private key. This may be performed using the digital signature methodology described with respect to FIG. 3, or may be used by other encryption methods known to those skilled in the art. After encrypting the message, the sender proceeds to step 925 where it sends the encrypted message, the original message, and the sender identity information to the institution. This may be performed over an open network, such as the Internet, where the sender is accessing via a computer, or it may be over a closed network where the sender is sending the encrypted message by way of a smart card at a terminal.

Proceeding to step 930, the institution receives the encrypted message, the original message, and sender identity information and automatically searches the database, using the sender identity information, to find the sender's public key. The public key that is associated with the sender identity information is then retrieved from the database. At step 930, the institution decrypts the encrypted message using the retrieved public key that was associated with the sender identity information provided in step 910.

Proceeding to step 940, the institution then validates the decrypted message with the original message sent. In one embodiment, the validation is performed using the digital signature validation paradigm previously described. After performing the validation, method 900 proceeds to step 945 and stops.

This validation process provides two purposes: (1) it determines whether the sender is the originator of the message because it is based on validation information provided by the sender to the institution; and (2) it validates the accuracy of the received message by detecting any changes to the message that was sent.

The present invention has been described in relation to particular embodiments which are intended in all respects to be illustrative rather than restrictive. Alternative embodiments will become apparent to those skilled in the art to which the present invention pertains without departing from its spirit and scope. Accordingly, the scope of the present invention is defined by the appended claims rather than the foregoing description.

\* \* \* \* \*

---

