A network-based sales system includes at least one buyer computer for operation by a user desiring to buy a product, at least one merchant computer, and at least one payment computer. The buyer computer, the merchant computer, and the payment computer are interconnected by a computer network. The buyer computer is programmed to receive a user request for purchasing a product, and to cause a payment message to be sent to the payment computer that comprises a product identifier identifying the product. The payment computer is programmed to receive the payment message, to cause an access message to be created that comprises the product identifier and an access message authenticator based on a cryptographic key, and to cause the access message to be sent to the merchant computer. The merchant computer is programmed to receive the access message, to verify the access message authenticator to ensure that the access message authenticator was created using the cryptographic key, and to cause the product to be sent to the user desiring to buy the product.

48 Claims, 25 Drawing Sheets

Microfiche Appendix Included
(1 Microfiche, 34 Pages)
OTHER PUBLICATIONS

Bo et al.; "SmartCash: A Practical Electronic Payment System"; pp. 1–8; Aug. 1990.
Dukach, Semyon; "SNPP: A Simple Network Payment Protocol"; MIT Laboratory for Computer Science; Cambridge, Massachusetts; 1993.

Intel Corporation; Power Technology; Marketig Brochure; no date.
Needham, Roger M.; "Adding Capability Access to Conventional File Servers"; Xerox Palo Alto Research Center; Palo Alto, California; no date.
Gifford, David K.; "Cryptographic Sealing for Information Secrecy and Authentication"; Stanford University and Xerox Palo Alto Research Center; Communications of the ACM; vol. 25, No. 4; Apr., 1982.
Mosaic Communications Corp; press release; "Mosaic Communications Unveils Network Navigator and Server Software for the Internet"; Sep. 12, 1994.
Tennenbaum, Jay M. and Schiffman, Allan M.; "Development of Network Infrastructure and Services for Rapid Acquisition"; adapted from a white paper submitted to DARPA by MCC in collaboration with EIT and ISI.
FIG. 1
user requests advertisements

buyer computer sends advertising document URL to merchant computer

merchants computer fetches advertising document from advertising document data base

merchant computer sends advertising document to buyer computer

user requests a product

buyer computer sends payment URL A to payment computer; payment URL A includes product identifier, domain identifier, payment amount, merchant computer identifier, merchant account identifier, duration time, expiration time, payment URL authenticator, and a buyer network address

payment computer verifies whether payment URL authenticator was created from contents of payment URL A using cryptographic key

payment computer sends document to buyer computer indicating that access to the network sales system is denied.

End

FIG. 2A
buyer computer 12  merchant computer 14  payment computer 16

payment computer checks whether expiration time has past

payment computer sends document indicating that expiration time has past

End

OR

payment computer checks to see if buyer network address in payment URL matches buyer's computer network address

OR

payment computer sends document indicating that access to network payment system is denied

FIG. 2B
buyer computer 12

payment computer sends payment confirmation document to buyer computer; payment confirmation document includes open link (URL C) and continue link (URL B)

46

user opens new account

44

payment computer 14

42

merchant computer 14

payment computer 16

58

payment computer sends payment URL B to payment computer; payment URL B is similar to payment URL A but also indicates that an account does exist

User continues with payment (user already has an account)

60

buyer computer sends payment URL C to payment computer; payment URL C is similar to payment URL A but also indicates that an account does not yet exist

54

payment computer creates new account document

52

payment computer sends new account document to buyer computer

FIG. 2C
buyer computer 12

user enters new account name, account password credit card number, security information and expiration date of credit card and presses a "submit" button

buyer computer sends new account information to payment computer

payment computer enters new account

payment computer creates account name and password request message

user enters account name and password

payment computer sends account name and password request message to buyer computer

buyer computer sends account name and password to payment computer

payment computer verifies whether user name and password are correct

payment computer sends document to buyer computer indicating that access to the networks sales system is denied

End

OR

FIG. 2D
user enters security information

payment computer determines whether additional security is warranted, based on, e.g., whether the payment amount exceeds a threshold

if additional security is warranted, payment computer creates a challenge form document and sends it to buyer computer

buyer computer sends security information to payment computer

payment computer determines whether security information is correct

payment computer sends document to buyer computer indicating that access to the network sales system is denied

End

FIG. 2E
buyer computer 12  merchant computer 14  payment computer 16

payment computer checks settlement database to determine if user has unexpired access to the domain identifier contained in the payment URL.

payment computer sends to buyer computer option to repurchase, or to use previously purchased access.

buyer selects to repurchase item

buyer selects previously purchased access

payment computer calculates an actual payment amount that may differ from the payment amount contained in the payment URL.

FIG. 2F
payment computer verifies whether user account has sufficient funds or credit

payment computer sends document to buyer computer indicating that user account does not have sufficient funds

payment computer creates access URL which includes merchant computer identifier, domain identifier, product identifier, end of duration time, buyer network address, and access URL authenticator

payment computer records product identifier, domain, user account, merchant account, end of duration time, and actual payment amount in settlement database

payment computer sends redirect to access URL to buyer computer

FIG. 2G
buyer computer 12  merchant computer 14  payment computer 16

buyer computer sends access URL to merchant computer

merchant computer verifies whether access URL authenticator was created from contents of access URL using a cryptographic key

merchant computer sends document to buyer computer indicating that access to the product is denied

End

OR

merchant computer verifies whether the duration time has expired

merchant computer sends document to buyer computer indicating that the duration time has expired

End

FIG. 2H
buyer computer 12  merchant computer 14  payment computer 16

merchant computer verifies that the buyer computer network address matches the network address specified in the access URL

 merchant computer sends document fulfillment document to buyer computer

buyer computer displays fulfillment document

End

End

FIG. 21
buyer computer 12

merchant computer 14

payment computer 16

From 32

buyer computer sends shopping cart URL to payment computer; shopping cart URL includes product identifier, domain identifier, payment amount, merchant computer identifier, merchant account identifier, duration time, expiration time, and shopping cart URL authenticator

payment computer verifies whether shopping cart URL authenticator was created from contents of shopping cart URL using a cryptographic key

payment computer sends document to buyer computer indicating that access to network sales system is denied

payment computer and buyer computer perform steps analogous to steps 40-81

End

FIG. 3A
buyer computer 12

user requests display of shopping cart

24

OR

user requests purchase of contents of shopping cart

116

buyer computer sends fetch shopping cart request to payment computer

118

merchant computer 14

payment computer 16

payment computer creates or updates payment URL for shopping cart

113

114

122

buyer computer displays shopping cart

124

buyer computer causes payment URL for shopping cart to be activated

126

payment computer and buyer computer perform steps analogous to steps 64-81

120

payment computer returns contents of shopping cart to buyer computer

119

to step 36

FIG. 3B
user requests smart statement

payment computer verifies whether smart statement URL authenticator was created from contents of smart statement URL using cryptographic key

payment computer sends document to buyer computer indicating that access is denied

payment computer checks to determine whether buyer network address in smart statement URL matches buyer's computer network address

payment computer sends document indicating that access is denied

payment computer and buyer computer perform steps analogous to steps 64-81

FIG. 4A
buyer computer 12  merchant computer 14  payment computer 16

buyer computer displays received document

User requests payment details for a particular transaction

buyer computer sends payment detail URL to payment computer

payment computer retrieves settlement data from settlement database and creates smart statement document for buyer and sends smart statement document to buyer computer

payment computer and buyer computer perform steps analogous to steps 132-140

payment computer retrieves from settlement database data corresponding to the payment transaction specified in the payment detail URL, creates detail document, and sends it to buyer computer

FIG. 4B
buyer computer 12

user requests customer service

buyer computer sends customer service URL to payment computer

user types comments

buyer computer sends user's comments to payment computer

user requests display of a product

buyer computer sends access URL to merchant computer

merchant computer 14

payment computer 16

FIG. 4C
Mead Data Central: Internet Information

November 28, 1993
LC's debut on the Internet: Library of Congress catalog on the

Text of Abstract of Article

VERONICA: A GOPHER NAVIGATIONAL TOOL ON THE INTERNET

October, 1993

FIG. 5
Open Market Payment

You have selected an item that requires payment

**Merchant:** Test Merchant  
**Description:** Mead Data Central Article  
**Amount:** $2.85 (US currency)

If you have an Open Market account click on "continue" below and you will be prompted for your account name and password. If you do not have an account, you can establish one on-line and return to this page to continue your purchase.

- Open an account on-line
- Continue with payment transaction.

**NOTE:** For demonstrations use the account name testuser@openmarket.com with the password testuser.

Open Market, Inc.

---

**FIG. 6**
Establish OpenMarket Account

Card Number: 
Expiration Date: (format MM/YY)

Check the appropriate boxes:
☐ I am the owner of the above credit card.
☐ The above address is also the billing address for this credit card.

Your OpenMarket account statement is available on-line. At your option you may a copy of your statement automatically sent to your e-mail address at weekly or monthly intervals. Please choose a statement option.

☐ Weekly statements   ☐ Monthly statements   ☐ No e-mail statements

Account name and password

Please choose an account name and password for your OpenMarket account. We suggest using an account name that is unique and easy to remember such as your e-mail address. Your password should be 8 characters or longer.

Account Name 
Password 

FIG. 7
Document is protected.
Enter username for Open Market Account at payment.openmarket.com:

FIG. 8

Cancel

OK
Open Market Payment

You have selected an item that you have purchased recently.

Merchant: Test Merchant
Description: Mead Data Central Article
Amount: 2.85 (US currency)

This could happen because you would like to buy the item again or it may have happened by accident.

You can:
- Go directly to the previous item
- Go ahead and buy the item again

Open Market, Inc.
LC's debut on the internet Library of Congress catalog

Text of Article

FIG. 10
**Transactions in October 1994**

<table>
<thead>
<tr>
<th>Date</th>
<th>Merchant</th>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Oct 3</td>
<td>Test Merchant</td>
<td>Dilbert subscription</td>
<td>$0.10</td>
</tr>
<tr>
<td>Tue Oct  4</td>
<td>Test Merchant</td>
<td>Mead Data Central Article</td>
<td>$2.95</td>
</tr>
<tr>
<td>Tue Oct  4</td>
<td>Test Merchant</td>
<td>Mead Data Central Article</td>
<td>$2.95</td>
</tr>
<tr>
<td>Tue Oct  4</td>
<td>Test Merchant</td>
<td>N.Y. Times Article</td>
<td>$0.50</td>
</tr>
<tr>
<td>Wed Oct  5</td>
<td>Test Merchant</td>
<td>Mead Data Central Article</td>
<td>$2.95</td>
</tr>
<tr>
<td>Wed Oct  5</td>
<td>Test Merchant</td>
<td>Mead Data Central Article</td>
<td>$2.95</td>
</tr>
<tr>
<td>Wed Oct  5</td>
<td>Test Merchant</td>
<td>Mead Data Central Article</td>
<td>$2.95</td>
</tr>
<tr>
<td>Wed Oct  5</td>
<td>Test Merchant</td>
<td>Mead Data Central Article</td>
<td>$2.95</td>
</tr>
</tbody>
</table>

Your total is $33.05.

**Previous Statements**

- September 1994
- August 1994

Return to your Newest Statement

**Feedback**

You can send us comments and suggestions here.
Smart Statement Detail

This is the detailed information about a particular transaction from your Smart Statement.

Transaction Information

- transaction_log_id: 50254.0
- currency: US
- transaction_date: 78177633
- initiator: 1.0
- expiration: 2592000
- description: Mead Data Central Article
- amount: 2.95
- beneficiary: 3.0
- ip_address: 199.170.183.13
- transaction_type: p
- domain: mead.internet-1

Merchant Information

- telephone: 617-621-9501
- address_1: Open Market, Inc.
- address_2: 215 First Street
- fax: 617-621-1703
- address_3: Cambridge, MA
- email: testmerchant@openmarket.com
- principal_name: Test Merchant

FIG. 12
Or if you prefer, you can send your comments via electronic mail to feedback@openmarket.com or via FAX to +1.617.621.1703. If you would like a reply please include your e-mail address.

Your Open Market account name (optional):

Your E-mail address (optional):

Subject:

Your comments:

Submit Feedback

FIG. 14
In one aspect, the invention features a network-based sales system that includes at least one buyer computer for operation by a user desiring to buy products, at least one merchant computer, and a payment computer to provide at least one server computer for operation by a client user and at least one server computer for operation by a server user. The client computer and the server computer are interconnected by a computer network. The session link message includes a session link authenticator, computed by a cryptographic function of the session link contents, for authenticating the session link message. The server computer is programmed to cause the session link message to be sent to the client computer. The client computer is programmed to cause the session link message to be sent to a computer in the network that is programmed to authenticate the session link message by examining the session link authenticator and that is programmed to respond to the session link message based on the state of the interaction between the client computer and the server computer.

In another aspect, the invention features a network-based link message system that includes at least one client computer for operation by a client user and at least one server computer for operation by a server user. The client computer and the server computer are interconnected by a computer network. The server computer is programmed to cause the session link message to be sent to the client computer. The client computer is programmed to cause the session link message to be sent to a computer in the network that is programmed to authenticate the session link message by examining the session link authenticator and that is programmed to respond to the session link message based on the state of the interaction between the client computer and the server computer.

In another aspect, the invention features a network-based link message system that includes at least one client computer for operation by a client user and at least one server computer for operation by a server user. The client computer and the server computer are interconnected by a computer network. The server computer is programmed to cause the session link message to be sent to the client computer. The client computer is programmed to cause the session link message to be sent to a computer in the network that is programmed to authenticate the session link message by examining the session link authenticator and that is programmed to respond to the session link message based on the state of the interaction between the client computer and the server computer.

The invention provides a simple design architecture for the network sales system that allows the merchant computer to respond to payment orders from the buyer computer without the merchant computer having to communicate directly with the payment computer to ensure that the user is authorized to purchase the product and without the merchant computer having to store information in a database regarding which buyers are authorized to purchase which products. Rather, when the merchant computer receives an access message from the buyer computer identifying a product to be purchased, the merchant computer need only check the access message to ensure that it was created by the payment computer (thereby establishing for the merchant computer that the buyer is authorized to purchase the product), and then the merchant computer can cause the product to be sent to the buyer computer who has been authorized to purchase the product.

In another aspect, the invention features a network-based link message system that includes at least one client computer for operation by a client user and at least one server computer for operation by a server user. The client computer and the server computer are interconnected by a computer network. The server computer is programmed to cause the session link message to be sent to the client computer. The client computer is programmed to cause the session link message to be sent to a computer in the network that is programmed to authenticate the session link message by examining the session link authenticator and that is programmed to respond to the session link message based on the state of the interaction between the client computer and the server computer.

In another aspect, the invention features a network-based link message system that includes at least one client computer for operation by a client user and at least one server computer for operation by a server user. The client computer and the server computer are interconnected by a computer network. The server computer is programmed to cause the session link message to be sent to the client computer. The client computer is programmed to cause the session link message to be sent to a computer in the network that is programmed to authenticate the session link message by examining the session link authenticator and that is programmed to respond to the session link message based on the state of the interaction between the client computer and the server computer.

In another aspect, the invention features a network-based link message system that includes at least one client computer for operation by a client user and at least one server computer for operation by a server user. The client computer and the server computer are interconnected by a computer network. The server computer is programmed to cause the session link message to be sent to the client computer. The client computer is programmed to cause the session link message to be sent to a computer in the network that is programmed to authenticate the session link message by examining the session link authenticator and that is programmed to respond to the session link message based on the state of the interaction between the client computer and the server computer.

In another aspect, the invention features a network-based link message system that includes at least one client computer for operation by a client user and at least one server computer for operation by a server user. The client computer and the server computer are interconnected by a computer network. The server computer is programmed to cause the session link message to be sent to the client computer. The client computer is programmed to cause the session link message to be sent to a computer in the network that is programmed to authenticate the session link message by examining the session link authenticator and that is programmed to respond to the session link message based on the state of the interaction between the client computer and the server computer.

In another aspect, the invention features a network-based link message system that includes at least one client computer for operation by a client user and at least one server computer for operation by a server user. The client computer and the server computer are interconnected by a computer network. The server computer is programmed to cause the session link message to be sent to the client computer. The client computer is programmed to cause the session link message to be sent to a computer in the network that is programmed to authenticate the session link message by examining the session link authenticator and that is programmed to respond to the session link message based on the state of the interaction between the client computer and the server computer.

In another aspect, the invention features a network-based link message system that includes at least one client computer for operation by a client user and at least one server computer for operation by a server user. The client computer and the server computer are interconnected by a computer network. The server computer is programmed to cause the session link message to be sent to the client computer. The client computer is programmed to cause the session link message to be sent to a computer in the network that is programmed to authenticate the session link message by examining the session link authenticator and that is programmed to respond to the session link message based on the state of the interaction between the client computer and the server computer.
plurality of digital advertisements and a plurality of respective product fulfillment items, at least one creation computer for creating the merchant database, and at least one merchant computer for causing the digital advertisements to be transmitted to a user and for causing advertised products to be transmitted to the user. The creation computer and the merchant computer are interconnected by a computer network. The creation computer is programmed to create the merchant database, and to transmit the digital advertisements and the product fulfillment items to the merchant computer. The merchant computer is programmed to receive the digital advertisements and product fulfillment items, to receive a request for a digital advertisement from a user, to cause the digital advertisement to be sent to the user, to receive from the user an access message identifying an advertised product, and to cause the product to be sent to the user in accordance with a product fulfillment item corresponding to the product.

In another aspect, the invention features a hypertext statement system that includes a client computer for operation by a client user and one or more server computers for operation by a server user. The client computer and the server computers are interconnected by a computer network. At least one of the server computers is programmed to record purchase transaction records in a database. Each of the purchase transaction records includes a product description. The server computer is programmed to transmit a statement document that includes the purchase transaction records to the client computer. The client computer is programmed to display the product descriptions, to receive a request from the client user to display a product corresponding to a product description displayed by the client computer, and to cause a product hypertext link derived from a purchase transaction record to be activated. At least one of the server computers is programmed to respond to activation of the product hypertext link by causing the product to be sent to the client computer. In another aspect, the invention features a network payment system that includes at least one buyer computer for operation by a user desiring to buy a product and at least one payment computer for processing payment messages from the buyer computer. The buyer computer and the payment computer are interconnected by a computer network. The buyer computer is programmed to cause a payment message to be sent to the payment computer. The payment message includes a product identifier identifying the product that the user desires to buy. The payment computer is programmed to receive the payment message, to cause an access message to be created to enable the user to access the product, and to record a purchase transaction record in the settlement database. The buyer computer is programmed to cause a request for purchase transaction records to be sent to the payment computer. The payment computer is programmed to receive the request for purchase transaction records and to cause a document derived from the purchase transaction records to be sent to the buyer computer.

**BRIEF DESCRIPTION OF THE DRAWINGS**

FIG. 1 is a block diagram of a network sales system in accordance with the present invention. FIG. 2 (2-A through 2-I) is a flowchart diagram illustrating the operation of a purchase transaction in the network sales system of FIG. 1. FIG. 3 (3-A through 3-B) is a flowchart diagram illustrating the use of a shopping cart for the purchase of products in connection with the network sales system of FIG. 1.

---

**FIG. 4** (4-A through 4-C) is a flowchart diagram illustrating the operation of a smart statement in the network sales system of FIG. 1.

**FIG. 5** is a screen snapshot of an advertising document that the merchant computer sends to the buyer computer in FIG. 2.

**FIG. 6** is a screen snapshot of a confirmation document that the payment computer sends to the buyer computer in FIG. 2.

**FIG. 7** is a screen snapshot of a new account document that the payment computer sends to the buyer computer in FIG. 2.

**FIG. 8** is a screen snapshot of an account name prompt that the buyer computer creates in FIG. 2.

**FIG. 9** is a screen snapshot of a document that the payment computer sends to the buyer computer in FIG. 2 and that provides an option either to repurchase or to use a previously purchased access.

**FIG. 10** is a screen snapshot of a fulfillment document that the merchant computer sends to the buyer computer in FIG. 2.

**FIG. 11** is a screen snapshot of a smart statement document that the payment computer sends to the buyer computer in FIG. 4.

**FIGS. 12 and 13** are screen snapshots of a transaction detail document that the payment computer sends to the buyer computer in FIG. 4.

**FIG. 14** is a screen snapshot of a customer service form that the payment computer sends to the buyer computer in FIG. 4.

**DETAILED DESCRIPTION**

With reference to FIG. 1, a network sales system in accordance with the present invention includes a buyer computer operated by a user desiring to buy a product, a merchant computer, which may be operated by a merchant willing to sell products to the buyer or by a manager of the network sales system, a payment computer typically operated by a manager of the network sales system, and a creation computer typically operated by the merchant. The buyer, merchant, payment, and creation computers are all interconnected by a computer network such as the Internet.

Creation computer is programmed to build a "store" of products for the merchant. A printout of a computer program for use in creating such a "store" in accordance with the present invention is provided as Appendix F.

The products advertised by merchant computer may be, for example, newspaper or newsletter articles available for purchase by buyers. Creation computer creates a digital advertisement database that stores advertising documents which may for example be in the form of summaries of newspaper or newsletter articles, accompanied by prices) and product fulfillment items which may be the products themselves if the products can be transmitted over the network, or which may be hard goods identifiers if the products are hard goods, i.e., durable products as opposed to information products). Creation computer transmits contents of the advertising document database to merchant computer to enable the merchant computer to cause advertisements and products to be sent to buyers. Merchant computer maintains advertising documents locally in advertising document database. In an alternative embodiment, the creation computer does not have a local digital advertisement database, but instead updates a remote
advertising document database on a merchant computer. These updates can be accomplished using HTML forms or other remote database technologies as is understood by practitioners of the art.

Payment computer 16 has access to a settlement database 22 in which payment computer 16 can record details of purchase transactions. The products may be organized into various "domains" of products, and payment computer 16 can access settlement database 22 to record and retrieve records of purchases of products falling within the various domains. Payment computer 16 also has access to a shopping cart database 21 in which a "shopping cart" of products that a user wishes to purchase can be maintained as the user shops prior to actual purchase of the contents of the shopping cart.

With reference to FIG. 2, a purchase transaction begins when a user at buyer computer 12 requests advertisements (step 24) and buyer computer 12 accordingly sends an advertising document URL (universal resource locator) to merchant computer 14 (step 26). The merchant computer fetches an advertising document from the advertising document database (step 28) and sends it to the buyer computer (step 30). An example of an advertising document is shown in FIG. 5. Details of URLs and how they are used are found in the microfiche Appendix G.

The user browses through the advertising document and eventually requests a product (step 32). This results in the buyer computer sending payment URL A to the payment computer (step 34). Payment URL A includes a product identifier that represents the product the user wishes to buy, a domain identifier that represents a domain of products to which the desired product belongs, a payment amount that represents the price of the product, a merchant computer identifier that represents merchant computer 14, a merchant account identifier that represents the particular merchant account to be credited with the payment amount, a duration time that represents the length of time for which access to the product is to be granted to the user after completion of the purchase transaction, an expiration time that represents a deadline beyond which this particular payment URL cannot be used, a buyer network address, and a payment URL authenticator that is a digital signature based on a cryptographic key. The payment URL authenticator is a hash of other information in the payment URL, the hash being defined by a key shared by the merchant and the operator of the payment computer.

In an alternative embodiment, step 34 consists of the buyer computer sending a purchase product message to the merchant computer, and the merchant computer provides payment URL A to the buyer computer in response to the purchase product message. In this alternative embodiment, payment URL A contains the same contents as above. The buyer computer then sends the payment URL A it has received from the merchant computer to the payment computer.

When the payment computer receives the payment URL it verifies whether the payment URL authenticator was created from the contents of the payment URL using the cryptographic key (step 36). If not, the payment computer sends a document to the buyer computer indicating that access to the network sales system is denied (step 38). Otherwise, the payment computer determines whether the expiration time has past (step 40). If it has, the payment computer sends a document to the buyer computer indicating that the time has expired (step 41). Otherwise, the payment computer checks the buyer computer network address to see if it matches the one specified in the payment URL (step 42). If it does not match, the payment computer sends a document to the buyer computer indicating that access to the network payment system is denied (step 43). Otherwise, the payment computer sends a payment confirmation document to the buyer computer, the payment confirmation document including an "open" link and a "continue" link (step 44).

An example of a confirmation document is shown in FIG. 6. The confirmation document asks the user to click on a "continue" button if the user already has an account with the payment computer, or to click on an "open" button if the user does not already have an account and wishes to open one.

If the user clicks on the "open" button (step 46), the buyer computer sends payment URL C to the payment computer (step 48), payment URL C being similar to payment URL A but also indicating that the user does not yet have an account.

The payment computer creates a new account document (step 50) and sends it to the buyer computer (step 52). An example of a new account document is shown in FIG. 7. When the user receives the new account document, the user enters the new account name, an account password, a credit card number, the credit card expiration date, and security information such as the maiden name of the user's mother (step 54), and presses a "submit" button (not shown in FIG. 7).

The buyer computer sends the new account information to the payment computer (step 56), which enters the new account in the settlement database (step 58).

If the user clicks on the "continue" button (step 60), the buyer computer sends payment URL B to the payment computer (step 62). Payment URL B being similar to payment URL A but also indicating that the user already has an account. The payment computer then instructs the buyer computer to provide the account name and password (steps 64 and 66), and the buyer computer prompts the user for this information by creating an account name prompt (example shown in FIG. 8) and a similar password prompt. The user enters the information (step 68) and the buyer computer sends the account name and password to the payment computer (step 70).

The payment computer verifies whether the user name and password are correct (step 72). If they are not correct, the payment computer sends a document to the buyer computer indicating that access to the network sales system is denied (step 74). Otherwise, the payment computer determines whether additional security is warranted, based on, e.g., whether the payment amount exceeds a threshold (step 73). If additional security is warranted, the payment computer creates a challenge form document and sends it to the buyer computer (step 75). The user enters the security information (step 77), the buyer computer sends the security information to the payment computer (step 79), and the payment computer determines whether the security information is correct (step 81). If it is not correct, the payment computer sends a document to the buyer computer indicating that access to the network sales system is denied (step 83).

If the security information is correct, or if additional security was not warranted, the payment computer checks the settlement database to determine whether the user has unexpired access to the domain identifier contained in the payment URL (step 82). If so, the payment computer sends a document to the buyer computer and provides an option either to repurchase or to use the previously purchased access (step 84). An example of such a document is shown in FIG. 9.
user can respond to the recent purchase query document by choosing to access the previously purchased document (step 85) or to go ahead and buy the currently selected product (step 86).

If the user chooses to access the previously purchased document, the buyer computer skips to step 92 (see below). If the user chooses to buy the currently selected product, the payment computer calculates an actual payment amount that may differ from the payment amount contained in the payment URL (step 87). For example, the purchase of a product in a certain domain may entitle the user to access other products in the domain for free or for a reduced price for a given period of time.

The payment computer then verifies whether the user account has sufficient funds or credit (step 76). If not, the payment computer sends a document to the buyer computer indicating that the user account has insufficient funds (step 78). Otherwise, the payment computer creates an access URL (step 80) that includes a merchant computer identifier, a domain identifier, a product identifier, an indicator that a product is to be granted, the buyer network address, and an access URL authenticator that is a digital signature based on a cryptographic key. The access URL authenticator is a hash of other information in the access URL, the hash being defined by a key shared by the merchant and the operator of the payment computer.

The payment computer then sends a redirect to access URL to the buyer computer (step 82), which sends the access URL to the merchant computer (step 82). The merchant computer verifies whether the access URL authenticator was created from the content of the access URL using the cryptographic key (step 84). If not, the merchant computer sends a document to the buyer computer indicating that access to the product is denied (step 86).

Otherwise, the merchant computer verifies whether the duration time for access to the product has expired (step 88). This is done because the buyer computer can request access to a purchased product repeatedly. If the duration time has expired, the merchant computer sends a document to the buyer computer indicating that the time has expired (step 90). Otherwise the merchant computer verifies that the buyer computer network address is the same as the buyer network address in the access URL (step 101), and if so, sends a fulfillment document to the buyer computer (step 102), which is displayed by the buyer computer (step 104). An example of a fulfillment document is shown in FIG. 10.

If the user chooses to print a key shared by the merchant and the operator of the payment computer.

The payment computer verifies whether the shopping cart URL authenticator was created from the contents of the shopping cart URL using a cryptographic key (step 110). If not, the payment computer sends a document to the buyer computer indicating that access to the network sales system is denied (step 112). Otherwise, before any modification to a user's shopping cart is allowed, user authentication is performed (step 113) in a manner analogous to steps 48-81. Once the user is authenticated, the payment computer creates or updates a payment URL for the shopping cart (step 114).

The user then either requests more advertisements (step 24 in FIG. 2) and possibly adds another product to the shopping cart, requests display of the shopping cart (step 116), or requests purchase of the entire contents of the shopping cart (step 124). If the user requests display of the shopping cart (step 116), the buyer computer sends a fetch shopping cart request to the payment computer (step 118), and the payment computer and buyer computer (step 119) perform steps analogous to steps 64-81. The payment computer returns the contents of the shopping cart to the buyer computer (step 120), which displays the contents of the shopping cart (step 122). If the user requests that the entire contents of the shopping cart be purchased (step 124) the payment computer causes the payment URL for the shopping cart to be activated (step 126) and the payment URL is processed in a manner analogous to the processing of payment URLs for individual products (beginning with step 36 in FIG. 2).

With reference now to FIG. 4, a user can request display of a "smart statement" that lists purchase transactions for a given month (step 128). When the buyer computer receives such a request, it sends a smart statement URL to the payment computer (step 130). When the payment computer receives the smart statement URL, it verifies whether the smart statement URL authenticator was created from the content of the smart statement URL using a cryptographic key (step 132). If not, the payment computer sends a document to the buyer computer indicating that access is denied (step 134). Otherwise, the payment computer checks to determine whether the buyer network address in the smart statement URL matches the buyer computer's actual network address (step 136). If not, the payment computer sends a document to the buyer computer indicating that access is denied (step 138). Otherwise (step 140), the payment computer and buyer computer perform a set of steps analogous to steps 64-81 in FIG. 2 (payment computer requests account name and password, user provides the requested information, and payment computer verifies the information).

In an alternative embodiment steps 132-138 are omitted. After verification of account information is complete, the payment computer retrieves the requested settlement data from the settlement database, creates a smart statement document for the buyer, and sends the smart statement document to the buyer computer (step 142). An example of a smart statement document is shown in FIG. 11. Each purchase transaction record in the smart statement document includes the data of the transaction, the name of the merchant, an identification of the product, and the payment amount for the product. The smart statement document also includes a transaction detail URL for each purchase transaction (these URLs or hypertext links, are discussed below and are not shown in FIG. 11). The smart statement docu-
The buyer computer displays the retrieved document (step 144), and the user may request transaction details for a particular transaction listed on the smart statement (step 146). If so, the buyer computer sends a transaction detail URL (or "payment detail URL") to the payment computer (step 148). The transaction detail URL includes a transaction identifier, a buyer network address, and a transaction detail URL authenticator. When the payment computer receives the transaction detail URL, it performs (step 150) a set of steps analogous to steps 132–140 (verification of URL authenticator, buyer network address, and account information). The payment computer then retrieves from the settlement database data corresponding to the payment transaction specified in the transaction detail URL, creates a transaction detail document, and sends it to the buyer computer (step 152).

An example of a transaction detail document is shown in FIGS. 12 and 13. The document displays a number of items of information about the transaction, including the transaction date, end of the duration time ("expiration"), a description of the product, the payment amount, the domain corresponding to the product, an identification of the merchant, and the merchant's address.

The smart statement document and the transaction detail document both include customer service URLs (hypertext links) that allow the user to request customer service (i.e., to send comments and suggestions to the payment computer). When the user requests customer service (step 154), the buyer computer sends the customer service URL to the payment computer (step 156), which creates a customer service form and sends it to the buyer computer (step 158). An example of a customer service form is shown in FIG. 14.

The user types comments into the customer service form (step 160), and the buyer computer sends the user's comments to the payment computer (step 162). The payment computer then posts the user comments and sends a thank you document to the buyer computer (step 164).

A user may request display of a product included in the smart statement. When the user requests that the product be displayed (step 166), the buyer computer sends the access URL contained in the smart statement document to the merchant computer (step 168), and the buyer computer and merchant computer perform a set of steps analogous to steps 94–104 in FIG. 2 (authentication of access URL, verification whether duration time has expired, verification of buyer network address, and transmission of fulfillment document to buyer computer).

Whenever the present application states that one computer sends a URL to another computer, it should be understood that in preferred embodiments the URL is sent in a standard HTTP request message, unless a URL message is specified as a redirection in the present application. The request message includes components of the URL as described by the standard HTTP protocol definition. These URL components in the request message allow the server to provide a response appropriate to the URL. The term "URL" as used in the present application is an example of a "link," which is a pointer to another document or form (including multimedia documents, hypertext documents including other links, or audio/video documents).

When the present application states that one computer sends a document to another computer, it should be understood that in preferred embodiments the document is a success HTTP response message with the document in the body of the message. When the present application states that a server sends an account name and password request message to the client, it should be understood that in preferred embodiments the account name and password request message is an unauthorized HTTP response. A client computer sends account name and password information to a server as part of a request message with an authorization field.

The software architecture underlying the particular preferred embodiment is based upon the hypertext conventions of the World Wide Web. Appendix A describes the Hypertext Markup Language (HTML) document format used to represent digital advertisements. Appendix B describes the HTML forms fill out support in Mosaic 2.0. Appendix C is a description of the Hypertext Transfer Protocol (HTTP) between buyer and merchant computers. Appendix D describes how documents are named with Uniform Resource Locators (URLs) in the network of computers, and Appendix E describes the authentication of URLs using digital signatures.

A printout of a computer program for use in creating and operating such a "store" in accordance with the present invention is provided as Appendix F. A printout of a computer program for use in operating other aspects of the network sales system in accordance with the present invention is provided in the microfiche appendix G.

There has been described a new and useful network-based sales system. It is apparent that those skilled in the art may make numerous modifications and departures from the specific embodiments described herein without departing from the spirit and scope of the claimed invention.

What is claimed is:
1. A network-based sales system, comprising:
   at least one buyer computer for operation by a user desiring to buy a product;
   at least one merchant computer; and
   at least one payment computer;
   said buyer computer, said merchant computer, and said payment computer being interconnected by a computer network;
   said buyer computer being programmed to receive a user request for purchasing a product, and to cause a payment message to be sent to said payment computer that comprises a product identifier identifying said product;
   said payment computer being programmed to receive said payment message, to cause an access message to be created that comprises said product identifier and an access message authenticator based on a cryptographic key, and to cause said access message to be sent to said merchant computer; and
   said merchant computer being programmed to receive said access message, to verify said access message authenticator to ensure that said access message was created using said cryptographic key, and to cause said product to be sent to said user desiring to buy said product.
2. A network-based sales system in accordance with claim 1, wherein said payment message and said access message each comprises a universal resource locator.
3. A network-based sales system in accordance with claim 1, wherein said payment computer is programmed to identify said merchant computer upon receipt of said payment message from said buyer computer.
4. A network-based sales system in accordance with claim 1, wherein said access message comprises a buyer network address.
5. A network-based sales system in accordance with claim 4, wherein:
   said product can be transmitted from one computer to another; and
   said merchant computer causes said product to be sent to said user by transmitting said product to said buyer network address only.

6. A network-based sales system in accordance with claim 4, wherein said merchant computer is programmed to verify whether said buyer network address in said access message matches the actual network address of said buyer computer.

7. A network-based sales system in accordance with claim 1, wherein said payment message comprises a buyer network address.

8. A network-based sales system in accordance with claim 7, wherein said payment computer is programmed to verify whether said buyer network address in said payment message matches the actual network address of said buyer computer.

9. A network-based sales system in accordance with claim 1, wherein said access message authenticator comprises a cryptographic function of contents of said access message based on said cryptographic key.

10. A network-based sales system in accordance with claim 1, wherein said payment message authenticator comprises a cryptographic function of contents of said payment message based on said cryptographic key.

11. A network-based sales system in accordance with claim 1, wherein said payment message comprises a payment amount.

12. A network-based sales system in accordance with claim 1, wherein said payment message comprises a payment amount.

13. A network-based sales system in accordance with claim 1, wherein said payment message comprises a merchant account identifier that identifies a merchant account.

14. A network-based sales system in accordance with claim 1, wherein said buyer computer is programmed to transmit a user account identifier to said payment computer that identifies a user account.

15. A network-based sales system in accordance with claim 14, wherein:
   said payment message comprises a payment amount; and
   said payment computer is programmed to ensure that said user account has sufficient funds or credit to cover said payment amount.

16. A network-based sales system in accordance with claim 14, wherein:
   said payment message comprises a payment amount and a merchant account identifier that identifies a merchant account; and
   said payment computer is programmed to record said payment amount, said user account, and said merchant account in a settlement database.

17. A network-based sales system in accordance with claim 16, wherein:
   said payment message comprises a domain identifier; and
   said payment computer is programmed to record said domain identifier and said user account in a settlement database.

18. A network-based sales system in accordance with claim 17, wherein said payment computer is programmed to check said settlement database, upon receipt of said payment message, to determine whether said user account has previously purchased a product associated with said domain identifier.

19. A network-based sales system in accordance with claim 18, wherein said payment computer is programmed to determine an actual payment amount for said product identified by said product identifier in said payment message based on whether said user account has previously purchased a product associated with said domain identifier.

20. A network-based sales system in accordance with claim 1, wherein said buyer computer is programmed to transmit a user authenticator to said payment computer and said payment computer is programmed to verify said user authenticator.

21. A network-based sales system in accordance with claim 20, wherein said user authenticator comprises a password.

22. A network-based sales system in accordance with claim 20, wherein:
   said buyer computer is programmed to transmit security information to said payment computer;
   said payment computer is programmed to transmit a challenge form to said buyer computer under a predetermined condition, said challenge form asking for said security information previously transmitted by said buyer computer to said payment computer; and
   said payment computer is programmed to verify authenticity of said security information.

23. A network-based sales system in accordance with claim 22, wherein:
   said payment message comprises a payment amount; and
   said predetermined condition comprises receipt of a payment amount in said payment message that exceeds a threshold.

24. A network-based sales system in accordance with claim 1, wherein said payment message comprises a merchant computer identifier that identifies said merchant computer.

25. A network-based sales system in accordance with claim 24, wherein said access message comprises said merchant computer identifier.

26. A network-based sales system in accordance with claim 1, wherein said payment message comprises a duration time that specifies a length of time for which access to said product is to be granted.

27. A network-based sales system in accordance with claim 26, wherein said payment computer is programmed to use said duration time to compute an end of duration time and to cause said end of duration time to be included in said access message.

28. A network-based sales system in accordance with claim 27, wherein said merchant computer is programmed to verify, upon receipt of said access message, that said end of duration time has not past.

29. A network-based sales system in accordance with claim 1, wherein said payment message comprises an expiration time after which said payment message can no longer be used.

30. A network-based sales system in accordance with claim 29, wherein said payment computer is programmed to verify, upon receipt of said payment message, that said expiration time has not past.

31. A network-based sales system in accordance with claim 1, wherein:
   said payment computer is programmed to cause said access message to be sent to said buyer computer; and
said buyer computer is programmed to cause said access message received from said payment computer to be sent to said merchant computer.

32. A network-based sales system, comprising:
at least one buyer computer for operation by a user desiring to buy a product; at least one merchant computer; and
said buyer computer, said merchant computer, and said payment computer being interconnected by a computer network;
said buyer computer being programmed to receive a user request for purchasing a product, and to cause a payment URL to be sent to said payment computer that comprises a product identifier identifying said product, a payment amount, and a payment URL authenticator comprising a cryptographic function of contents of said payment URL based on a cryptographic key;
said payment computer being programmed to receive said payment URL, to verify said payment URL authenticator to ensure that said payment URL authenticator was created using said cryptographic key, to ensure that said user has sufficient funds or credit to cover said payment amount, to identify said merchant computer operated by said merchant willing to sell said product to said buyer, to cause an access URL to be created that comprises said product identifier and an access URL authenticator comprising a cryptographic function of contents of said access URL based on a cryptographic key, and to cause said access URL to be sent to said buyer computer;
said buyer computer being programmed to cause said access URL received from said payment computer to be sent to said merchant computer; and
said merchant computer being programmed to receive said access URL, to verify said access URL authenticator to ensure that said access URL authenticator was created using said cryptographic key, and to cause said product to be sent to said user desiring to buy said product.

33. A method of operating a payment computer in a computer network comprising at least one buyer computer for operation by a user desiring to buy a product, at least one merchant computer, and at least one payment computer, the method comprising the steps of:
receiving, at said payment computer, a payment message that said buyer computer has caused to be sent to said payment computer in response to a user request for purchasing a product, said payment message comprising a product identifier identifying said product;
causing an access message to be created that comprises said product identifier and an access message authenticator based on a cryptographic key; and
causing said access message to be sent to said merchant computer, said merchant computer being programmed to receive said access message, to verify said access message authenticator to ensure that said access message authenticator was created using said cryptographic key, and to cause said product to be sent to said user desiring to buy said product.

34. A network-based sales system, comprising:
at least one buyer computer for operation by a user desiring to buy products;
at least one shopping cart computer; and
a shopping cart database connected to said shopping cart computer;
said buyer computer and said shopping cart computer being interconnected by a computer network;
said buyer computer being programmed to receive a plurality of requests from a user to add a plurality of respective products to a shopping cart in said shopping cart database, and, in response to said requests to add said products, to send a plurality of respective shopping cart messages to said shopping cart computer each of which comprises a product identifier identifying one of said plurality of products;
said shopping cart computer being programmed to receive said plurality of shopping cart messages, to modify said shopping cart in said shopping cart database to reflect said plurality of requests to add said plurality of products to said shopping cart, and to cause a payment message associated with said shopping cart to be created; and
said buyer computer being programmed to receive a request from said user to purchase said plurality of products added to said shopping cart and to cause said payment message to be activated to initiate a payment transaction for said plurality of products added to said shopping cart;
said shopping cart being a stored representation of a collection of products, said shopping cart database being a database of stored representations of collections of products, and said shopping cart computer being a computer that modifies said stored representations of collections of products in said database.

35. A network-based sales system in accordance with claim 34, wherein said shopping cart computer is programmed to cause said payment message to be created before said buyer computer causes said payment message to be activated.

36. A network-based sales system in accordance with claim 34, wherein said buyer computer is programmed to receive a request from said user to display said plurality of products added to said shopping cart.

37. A network-based sales system in accordance with claim 36, wherein said buyer computer is programmed to transmit a fetch shopping cart request to said payment computer in response to receipt of said request from said user.

38. A network-based sales system in accordance with claim 37, wherein:
said payment computer is programmed to respond to said fetch shopping cart request by transmitting a message to said buyer computer indicating said plurality of products added to said shopping cart; and
said buyer computer is programmed to display said plurality of products added to said shopping cart.

39. A method of operating a shopping cart computer in a computer network comprising at least one buyer computer for operation by a user desiring to buy products, at least one shopping cart computer, and a shopping cart database connected to said shopping cart computer, the method comprising the steps of:
receiving, at said shopping cart computer, a plurality of shopping cart messages sent to said shopping cart computer by said buyer computer in response to receipt of a plurality of requests from a user to add a plurality of respective products to a shopping cart in said shopping cart database, each of said shopping cart messages comprising a product identifier identifying one of said plurality of products;
modifying said shopping cart in said shopping cart database to reflect said plurality of requests to add said plurality of products to said shopping cart; and
15. A method of operating a server computer in a network-based link message system comprising:

- at least one client computer for operation by a client user;
- and
- at least one server computer for operation by a server user;
- said client computer and said server computer being interconnected by a computer network;
- said client computer being programmed to send an initial link message to said server computer;
- said server computer being programmed to receive said initial link message from said client computer, to create, based on information contained in said initial link message, a session link message that encodes a state of interaction between said client computer and said server computer, said session link message comprising a session link authenticator, computed by a cryptographic function of said session link contents, for authenticating said session link message, and to cause said session link message to be sent to said client computer;
- said client computer being programmed to cause said session link message to be sent to a computer in said network that is programmed to authenticate said session link authenticator and that is programmed to respond to said session link message based on said state of said interaction between said client computer and said server computer.

41. A network-based link message system in accordance with claim 40, wherein:

- said client computer comprises a buyer computer for operation by a user desiring to buy a product;
- said server computer comprises a payment computer for operation by a manager of said network-based link message system; and
- said network-based link message system further comprises a merchant computer for operation by a merchant willing to sell said product to said buyer.

42. A network-based link message system in accordance with claim 41, wherein said computer that is programmed to cause a payment message associated with said shopping cart to be created;

- said buyer computer being programmed to receive a request from said user to purchase said plurality of products added to said shopping cart and to cause said payment message to be activated to initiate a payment transaction for said plurality of products added to said shopping cart;

- said shopping cart being a stored representation of a collection of products, said shopping cart database being a database of stored representations of collections of products, and said shopping cart computer being a computer that modifies said stored representations of collections of products in said database.

43. A network-based link message system in accordance with claim 41, wherein said initial link message comprises a payment message to said payment computer that comprises a product identifier identifying said product.

44. A network-based link message system in accordance with claim 43, wherein said session link message comprises an access message that comprises said product identifier to be created.

45. A network-based link message system in accordance with claim 44, wherein said merchant computer is programmed to respond to said access message by causing said product to be sent to said user desiring to buy said product.

46. A network-based link message system in accordance with claim 40, wherein said initial link message and said session link message comprise universal resource locators.

47. A network-based link message system in accordance with claim 40, wherein:

- said session link authenticator comprises a cryptographic function of contents of said session link message based on a cryptographic key; and
- said computer to which said client computer is programmed to cause said session link message to be sent is programmed to verify that said session link authenticator was created using said cryptographic key.

48. A method of operating a server computer in a network-based link message system comprising at least one client computer for operation by a client user and at least one server computer for operation by a server user, said client computer and said server computer being interconnected by a computer network, said method comprising the steps of:

- receiving, at said server computer, an initial link message sent to said server computer by said client computer;
- creating, based on information contained in said initial link message, a session link message that encodes a state of interaction between said client computer and said server computer, said session link message comprising a session link authenticator, computed by a cryptographic function of said session link contents, for authenticating said session link message; and
- causing said session link message to be sent to said client computer.

49. A method of operating a server computer in a network-based link message system comprising at least one client computer for operation by a user desiring to buy a product, said server computer comprising a payment computer for operation by a manager of said network-based link message system; and

- said network-based link message system further comprises a merchant computer for operation by a merchant willing to sell said product to said buyer.

* * * * *
On petition requesting issuance of a certificate for correction of inventorship pursuant to 35 U.S.C. 256, it has been found that the above identified patent, through error and without any deceptive intent, improperly sets forth the inventorship.

Accordingly, it is hereby certified that the correct inventorship of this patent is: Andrew C. Payne, Lincoln, MA; Lawrence C. Stewart, Burlington, MA; and G. Winfield Treese, Wayland, MA.

Signed and Sealed this Sixth Day of April 2004.

THOMAS H. TARCZA
Supervisory Patent Examiner
Art Unit 3662