(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2002 (24.01.2002)

PCT

(10) International Publication Number
WO 02/07493 A2

(51) International Patent Classification[7]: H06F

(21) International Application Number: PCT/EP01/07568

(22) International Filing Date: 3 July 2001 (03.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/615,878 13 July 2000 (13.07.2000) US

(71) Applicant: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: **EPSTEIN, Michael**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **GROENENDAAL, Antonius, W., M.**; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/07493 A2

(54) Title: AUDITING SYSTEM FOR E-COMMERCE VIA CONSUMER APPLIANCE

(57) Abstract: A receipt-signing and receipt-storage capability are integrated into consumer appliances that are used to effect secure purchases or purchase agreements. Set-top boxes having a "Buy" button, for example, are configured to store a digitally-signed receipt during each secure "buy" transaction. Electronic "wallets" that are commonly used on a personal computer or palmtop computer to effect secure purchases are similarly configured to store a digitally-signed receipt corresponding to each transaction. The receipts may be stored locally at the transaction device, or at "Receipt Warehouse" sites on the Internet. Each transaction device is assigned a public/private key pair by the manufacturer of the device. The manufacturer of the transaction device provides a digitally-signed copy of the public key, so that its authenticity can be verified. When a transaction is completed, the transaction device receives a copy of the purchase receipt or the purchase agreement, digitally signs it, and stores it for future access. When and if a dispute arises, the digitally signed receipts or agreements can be presented as evidence of the transaction. Because the transaction device effects this signing automatically upon receipt of the information via a secure connection, these digitally signed receipts and agreements should reduce the time and cost of resolving disputes by providing a verifiable record of the transaction.

Auditing System for E-Commerce via Consumer Appliance

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the field of electronic commerce, and in particular to an auditing system that facilitates dispute resolution.

2. Description of Related Art

Electronic commerce continues to expand, and technologies continue to be developed to prevent fraud and other deceitful acts. For example, most financial transactions occur via a "secure socket", wherein the identity of each participant in the transaction is verified.

One of the difficulties of electronic commerce is the absence of a "hard copy" of a receipt or purchase agreement. Agreements are made electronically, and electronic documents are often communicated between the buyer and seller, but such electronic documents can be easily modified by either party. When a subsequent dispute arises between the buyer and seller, the lack of a verifiable receipt often complicates the matter, and requires additional time and cost to resolve the issue.

Techniques are commonly available that facilitate the verification of an electronic document's authenticity. Such techniques are commonly termed "digital signing". When an electronic document is electronically signed by a party, using a secret key, the document can be certified as being signed by that party, because only that party knows the secret key. The digital signature is also dependent on the contents of the document, as well as the secret key. If the document is modified, the digital signature no longer corresponds to the contents of the modified document. Checksums, hash functions, and the like are commonly used to provide a digital signing process that has the above author-authentication and modification-detection characteristics.

Digital signing traditionally requires an overt act. In a typical electronic transaction, the seller would be responsible for digitally signing the receipt, and then the buyer would be responsible for digitally signing an acknowledgement of the receipt. In addition to the difficulty of assuring that each vendor and each purchaser will effect this

signing process, such a system would, in general, require that each vendor and purchaser use compatible digital signing and verification processes.

BRIEF SUMMARY OF THE INVENTION

It is an object of this invention to provide a method and apparatus that facilitates the verification of purchase receipts or purchase agreements. It is a further object of this invention to provide a method and apparatus that automates the digital signing process, thereby eliminating the need for overt actions to effect a verifiable audit trail. It is a further object of this invention to integrate this digital-signing process into the capabilities of newer consumer appliances.

These objects and others are achieved by integrating a receipt-signing and receipt-storage capability into consumer appliances that are used to effect purchases or purchase agreements. Set-top boxes having a "Buy" button, for example, are configured to store a digitally-signed receipt during each secure "buy" transaction. Electronic "wallets" that are commonly used on a personal computer or palmtop computer to effect secure purchases are similarly configured to store a digitally-signed receipt corresponding to each transaction. The receipts may be stored locally at the transaction device, or at "Receipt Warehouse" sites on the Internet. Each transaction device is assigned a public/private key pair by the manufacturer of the device. The manufacturer of the transaction device provides a digitally-signed copy of the public key, so that its authenticity can be verified. When a transaction is completed, the transaction device receives a copy of the purchase receipt or the purchase agreement, digitally signs it, and stores it for future access. When and if a dispute arises, the digitally signed receipts or agreements can be presented as evidence of the transaction. Because the transaction device effects this signing automatically upon receipt of the information via a secure connection, these digitally signed receipts and agreements should reduce the time and cost of resolving disputes by providing a verifiable record of the transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

FIG. 1 illustrates an example flow diagram of a transaction and corresponding storage of a digitally signed receipt in accordance with this invention.

FIG. 2 illustrates an example transaction device in accordance with this invention.

Throughout the drawings, the same reference numerals indicate similar or corresponding features or functions.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates an example flow diagram of a secure transaction 100 and corresponding storage of a digitally signed receipt 150 in accordance with this invention. A seller 20 provides an offer of sale 110. This offer 110 may be an advertisement in a newspaper, at a web-site, on a radio or television program, and so on. The offer 110 may also be an implicit offer. Copending U.S. patent application "Method and System for Purchasing Content Related Material", U.S. serial number 09/498,261, filed 3 February 2000 for Nicholas Mankovich, Michael Epstein, and Toine Staring, attorney docket US000036, discloses a method and system for purchasing items related to material being received from a broadcast, such as a song or advertisement being received by a radio. Activating a "buy button" while the material is being broadcast effects the purchase of the item being broadcast, such as a song, or an item associated with the broadcast, such as the item being advertised. In this environment, the broadcast of the song constitutes an offer of sale of the song by the party to whom the purchase request is sent. Other means of conveying a willingness to accept a purchase request are common in the art.

In accordance with this invention, a buyer 10 initiates a purchase request 120, via a transaction device 200. This transaction device 200 may include an appliance such as a radio, television, set-top box, and the like, that is equipped with the aforementioned "buy button" of the referenced copending patent application. The transaction device 200 may be a computer that includes an application program that facilitates on-line purchases from the Internet. Such application programs are often referred to as "electronic-wallets", and typically contain such information as the user's credit card number, billing and shipping addresses, and the like. The transaction device 200 may also include a personal "swipe machine" that the user uses to "swipe" a credit card to effect a purchase; this swipe machine may be attached to a conventional telephone, a fax machine, a computer, a set-top box, and so on. The transaction device 200 may be a conventional telephone with a capability of distinguishing transaction information, as discussed further below. As is common in the art, the transaction device 200 effects the purchase request via a "secure socket", that verifies the participants to the transaction. The buyer is assured that the party at the other end of the communication is

the identified seller, and/or an authorized agent of the seller, and the seller is assured that the buyer is authorized to effect the transaction, via, for example, the use of a user-name and PIN (Personal Identification Number) or other identifier of the buyer, such as a valid credit card number and expiration date. Other devices and techniques that facilitate the execution of a secure purchase request by a user are common in the art, and the application of this invention to such devices will be evident to one of ordinary skill in the art in light of this disclosure.

The seller 20 receives the purchase request 120, and if the request is acceptable to the seller 20, the seller 20 transmits a receipt 130. Note that the purchase request 120 may include a "reverse-bid" offer wherein the buyer communicates an offer to pay a given amount for an item to one or more sellers of the item, and the transaction continues with the first seller that is willing to accept the offered amount. In accordance with this invention, the receipt 130 is communicated to the buyer 10 in an electronic form that can be processed directly by the transaction device 200, without intervention by the buyer 10. For ease of reference, the receipt 130 is assumed herein to be the "final receipt" of the transaction 100. In those cases where the user has a subsequent option to accept or reject the terms specified in the response from the seller 20 to the user's purchase request 120, the response from the seller 20 is considered a counter-offer, or a new sales offer 110. As used herein, the "receipt" 130 represents the buyer's and seller's mutual acknowledgement of the purchase. Note that although an electronic document is a preferred form of the receipt 130, the receipt 130 could be a voice recording of the seller's acknowledgement of the purchase during a telephone transaction. In such an embodiment, the user's telephone would be configured to initiate the recording upon command by the buyer 10, or, if standards are established, could be triggered by a signal embedded in the telephonic signal, and so on. Preferably, the receipt 130 contains a reliable identifier of the seller 10, and a verification that the receipt 130 was received via a secure socket with the seller. Upon receiving the receipt 130, the transaction device 200 is configured, in accordance with this invention, to digitally sign the receipt 130, and to store this digitally signed receipt 150 in a data base 160 for subsequent retrieval if necessary. This digitally signed receipt 150 may contain ancillary information, such as the date and time of the reception, or other items that facilitate a retrieval of the information, or that facilitate a further verification of the receipt.

The transaction device 200 signs the receipt 130 using a private key 201 that is secret to the device 200, thus creating a signed receipt 170. In a preferred embodiment, this private key 201 is a private key of a public-private key pair that is allocated to the transaction device 200 by the manufacturer of the transaction device 200. The manufacturer also

provides the transaction device 200 with a digitally signed copy of the public key 202 corresponding to this private key 201. The digital signing of the public key 202 serves to verify the transaction device 200 as a "certified" transaction device 200. In accordance with the principles of this invention, the transaction device 200 is configured to automatically sign and store the receipt 130, without allowing the buyer 10 to modify the contents of the receipt 130. Using techniques common in the art, the transaction device 200 is also configure to preclude the certification of a receipt 130 if the device 200 has been tampered with.

FIG. 2 illustrates an example transaction device 200 in accordance with this invention. The transaction device 200 includes a secure channel transceiver 210 that effects a secure communication between the buyer and seller, such that each party is assured of the other party's identity. A protocol establishes the communication, using for example a user-name, account number, or other identification technique; thereafter, if the communication between the buyer and seller is interrupted during a transaction, the transaction is terminated. This provides a substantially continuous authentication of the parties to each transaction. The secure channel is initiated upon receipt of a purchase request from a buy device 220 in response to a user input. When the transaction is finalized, the seller communicates a receipt 130 via the secure channel transceiver 210, which is presented to the user upon command. At the same time, a signing device 230 signs the receipt 130, using the private key 201, and stores the signed receipt in a secure storage device 250. Note that because this receipt is communicated via the secure channel transceiver, the seller cannot deny having sent the receipt.

A verification device 260 provides a certified receipt 170 of the original receipt 130 upon demand. For example, the "demand" may be a court order, a request from the seller, a request from an arbitrator, and so on. The signed copy of the original receipt 130 is provided, which can be certified by verifying the signature using the transaction device's public key 202. Because the signing device 230 signs the receipt and stores it in a secure storage 240, without user intervention, neither the buyer nor seller can deny its authenticity.

A tamper detection device 280 is configured to preclude the generation of the certified receipt 170 if the security of the transaction device 200 is breached. For example, the storage device 250 may be a frangible device that is rendered inoperative if the casing to the device 200 is opened. Similarly, the verification device can be configured to provide a warning with each certified receipt 170 if a tamper has been detected.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which,

although not explicitly described or shown herein, embody the principles of the invention and are thus within its spirit and scope. For example, the transaction device 200 may also be configured to sign and store other parts of the transaction 100, including an entirety of the transaction 100. In a preferred embodiment, the transaction device 200 stores a copy of all of the user's purchase requests 120 in the data base 160, regardless of whether a receipt 130 was received. Preferably, each communication includes a date-time stamp, to correlate the transaction sequence. In this manner, the data base 160 can be used to verify the absence of a completed transaction 100, or the absence of a mutually agreed upon set of terms corresponding to a purchase request 120. In such an application, the data base 160 is configured to prevent the deletion of any signed receipts, or the transaction device 200 is configured to explicitly include an indication in the signed purchase request 120 whether a response was received. These and other system configuration and optimization features will be evident to one of ordinary skill in the art in view of this disclosure, and are included within the scope of the following claims.

CLAIMS:

1. A method of facilitating an audit of a transaction, comprising:

enabling a secure communication of a purchase request (120) from a first party to a second party,

enabling a receipt (130) from the second party, corresponding to an acceptance of the purchase request (120),

enabling an autonomous digital signing of the receipt (130) by a device associated with the first party, upon receipt of the receipt (130), to produce a digitally signed receipt (150), and

enabling a storage of the digitally signed receipt (150) corresponding to the transaction (100).

2. The method of claim 1, further including

enabling a retrieval of the digitally signed receipt (150) to facilitate a conflict resolution concerning the transaction (100).

3. The method of claim 1, further including

enabling an autonomous digital signing and storage of other communications related to the transaction (100).

4. The method of claim 1, further including:

enabling a presentation of content material, and

enabling the communication of the purchase request (120) in response to the presentation of the content material.

5. The method of claim 1, wherein

the autonomous digital signing is based on a private key (201) that is associated with the transaction device (200), and

the method further includes

enabling a verification of the digitally signed receipt (150) based on a public key (202) that is associated with the transaction device (200).

6. The method of claim 5, wherein

the private key (201) and public key (202) are associated with the transaction device (200) by a manufacturer of the transaction device (200), and

the method further includes

enabling a communication of a certified copy of the public key (202) to the second party, the certified copy being certified by the manufacturer of the transaction device (200).

7. The method of claim 1, wherein

enabling a storage of the digitally signed receipt (150) includes:

enabling an Internet access for storing the digitally signed receipt (150).

8. The method of claim 1, further including

enabling a date-time assocation with at least one of the purchase request (120) and the receipt (130).

9. A transaction device (200) comprising:

a transmission device that is configured to securely communicate a purchase request (120) from a first party to a second party,

a reception device that is configured to receive a receipt (130) from the second party, corresponding to an acceptance of the purchase request (120),

a signing device, operably coupled to the reception device, that is configured to:

provide a digitally signed receipt (150) corresponding to the receipt (130) that is received, and

store the digitally signed receipt (150) for subsequent retrieval.

10. The transaction device (200) of claim 9, further including:

a verification device that is configured to certify the digitally signed receipt (150) to facilitate a conflict resolution concerning the purchase request (120) and the acceptance of the purchase request (120).

11. The transaction device (200) of claim 10, wherein

the signing device is configured to provide the digitally signed receipt (150) based on a private key (201) that is associated with the transaction device (200), and

the verification device is configured to certify the digitally signed receipt (150) by communicating a public key (202) that is associated with the transaction device (200) and the digitally signed receipt (150) to a verification device.

12. The transaction device (200) of claim 11, wherein

the private key (201) and public key (202) are associated with the transaction device (200) by a manufacturer of the transaction device (200), and

the verification device communicates the public key (202) as a certified copy of the public key (202), the certified copy being certified by the manufacturer of the transaction device (200).

13. The transaction device (200) of claim 9, wherein

the reception device is configured to receive other documents relating to the purchase request (120) and the acceptance, and

the signing device is configured to digitally sign and store the other documents.

14. The transaction device (200) of claim 9, further including:

a renderer that is configured to provide a rendering of content material,

a buy device that is configured to initiate the purchase request (120) based on the content material.

15. The transaction device (200) of claim 9, further including:

an Internet access device, operably coupled to the signing device, that is configured to:

receive the digitally signed receipt (150) from the signing device, and

communicate the digitally signed receipt (150) via the Internet for storage.

16. The transaction device (200) of claim 9, further including:

a storage device, operably coupled to the signing device, that is configured to receive the digitally signed receipt (150) from the signing device for storage.

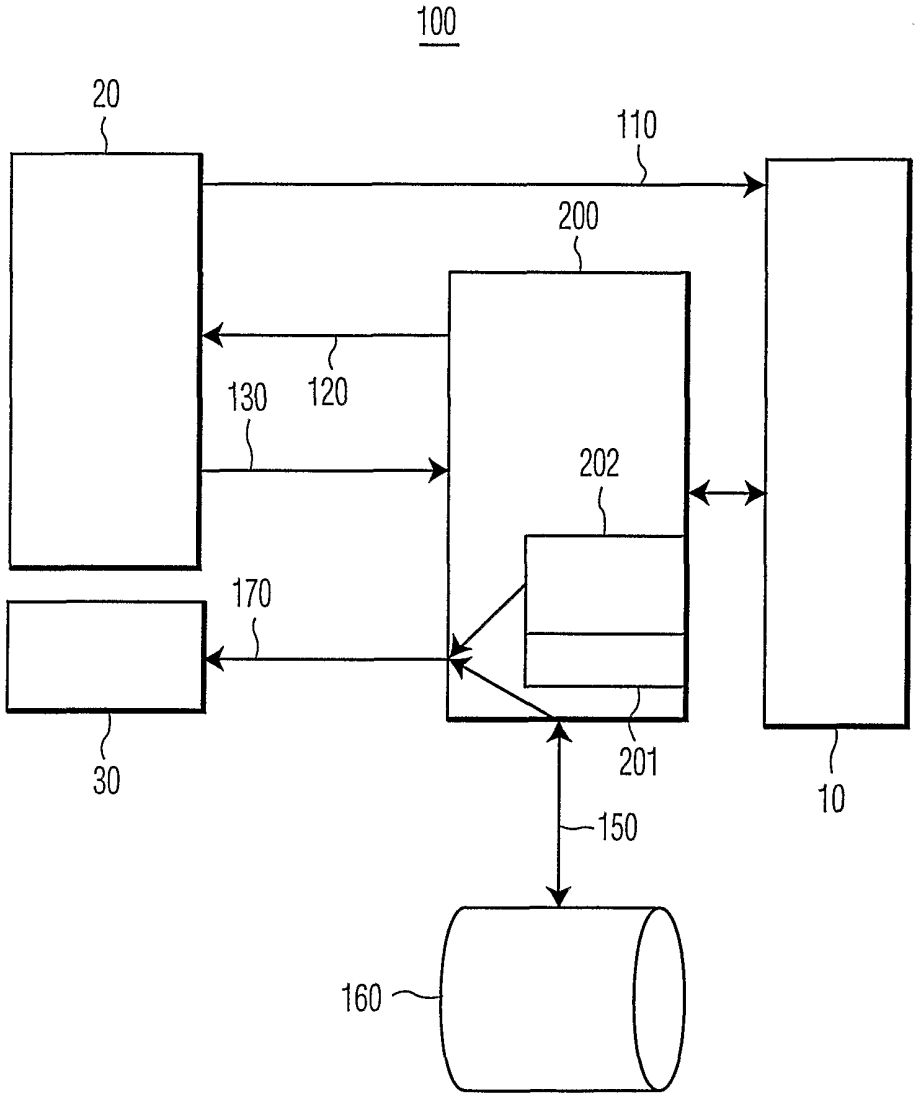

FIG. 1

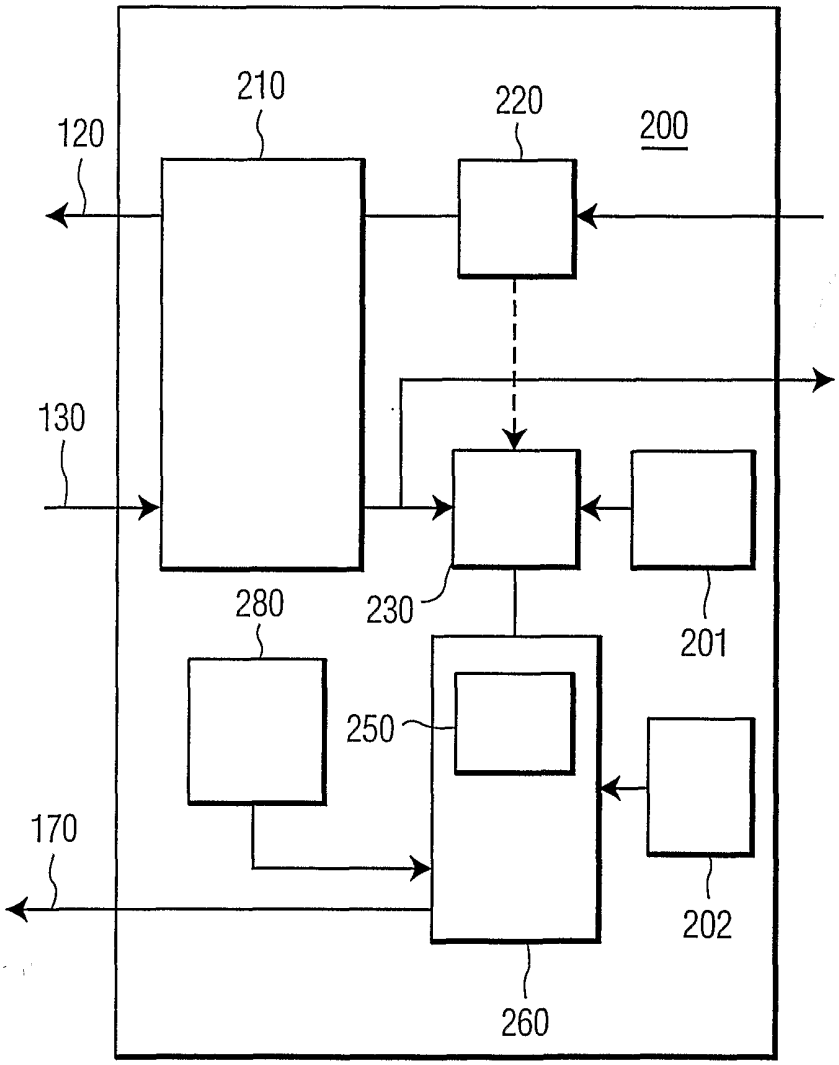

FIG. 2