

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
31 December 2008 (31.12.2008)

PCT

(10) International Publication Number
WO 2009/002517 A1

(51) International Patent Classification:
H04K 1/00 (2006.01)

(21) International Application Number:

PCT/US2008/007921

(22) International Filing Date: 23 June 2008 (23.06.2008)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

60/945,909

23 June 2007 (23.06.2007)

US

(71) Applicant and

(72) Inventor: ADAMS, Mark, W. [US/US]; 1700 St. Anthony Drive, San Jose, CA 95125 (US).

(74) Agent: HUGHES, Michael, J.; IPLO Intellectual Property Law Offices, 100 West San Fernando Street, suite 365, San Jose, CA 95113 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA,

CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

— with international search report

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

(54) Title: PAPERLESS TRANSACTION SYSTEM

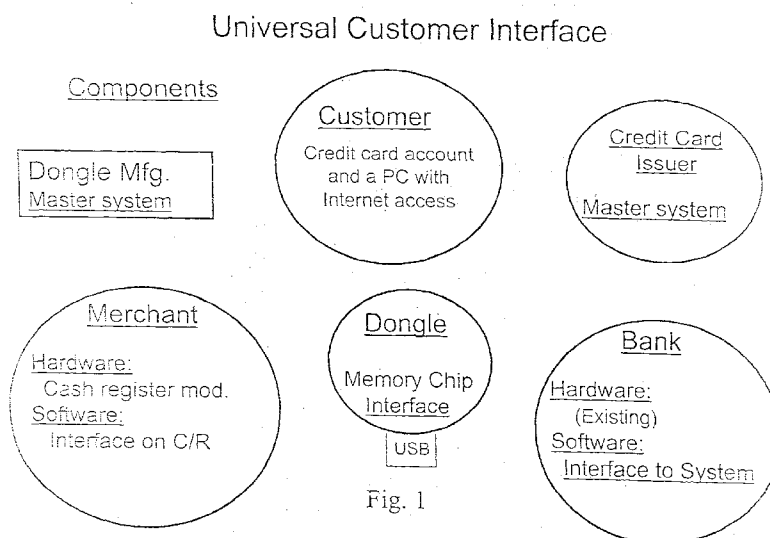


Fig. 1

(57) Abstract: A paperless transaction system (10) is provided for use as a universal customer interface utilized to engage in purchase and financial transactions (11). The system (10) includes an institutional subsystem (12) and a consumer subsystem (14) which interact through dataports (30), either physical or wireless. The consumer subsystem includes a user-carried dongle (74) having a memory component (76) for storing relevant information (50, 52, 54). Engaging dongle (74) with a TIST (22) of the institution acts to disable printers (26) and instead generates an electronic transaction record (38) stored in the dongle (74). Security is provided by a PIN (58) or biological identifier device (62) specific to the user.

WO 2009/002517 A1

PAPERLESS TRANSACTION SYSTEM

[0001] This application claims priority from the United States provisional application of the same general title, filed on 23 June 2007 as application No. 60/945,909.

TECHNICAL FIELD

[0002] The present invention relates generally to electronic transaction devices, whether direct or wireless, and particularly to ATM machines, cash registers and remote electronic transaction systems (Internet) and to consumer personal devices for interfacing therewith.

BACKGROUND ART

[0003] A great deal of paper is wasted every day by consumers engaging in transactions, be they purchases at the grocery store, deposits or withdrawals at the bank or numerous other financial transactions. In nearly every transaction, a paper receipt is printed and provided to the customer/client at the end. Although these are occasionally useful for immediate review or for purposes of showing purchase information to exit security guards, this is infrequently the case. In most cases the receipt, often half a meter or greater in length, is simply glanced at and discarded into the nearest trash bin, rarely even into recycling bins. This results in a great deal of waste disposal and unnecessary printing and paper costs.

[0004] In most cases, the transactions are handled and recorded by computers or computer powered devices such as automated teller machines (ATMs) or cash registers. These devices frequently download information on the transaction into databases, which may in some limited circumstances cases be accessed by the consumer. However, electronic records of most transactions are not available, at least in any detail, to the user.

[0005] The development of debit/credit cards which may be swiped for speedy transactions has resulted in a demand for increasing the fluidity and speed of purchasing. However, such methods have disadvantages in terms of security (anyone can use the card) and do nothing to address the paper reduction or transaction recording issues.

[0006] Online and wireless transactions are often hampered by the cumbersome and marginally effective procedures necessary to provide consumer credit information. It is not desirable for the consumer to provide each online merchant or service provider with sensitive information over the internet, but it is inconvenient to avoid this while providing for purchase transactions.

[0007] Accordingly, it is highly desirable to provide electronic data reflecting the content of transactions to the consumer. Further, any way to minimize the immense cost of paper and printing materials and technology would be a great benefit to both the consumer and the institution, not to mention the environment. Additionally, there is a continuing need to provide increased rapidity of transactions and security of sensitive user information. There is thus a great need and desire for methods to streamline transaction recording and availability to the consumer while reducing cost to the providers.

DISCLOSURE OF INVENTION

[0008] Accordingly, it is an object of the present invention to provide a method for providing transaction information to consumers without using paper tallies.

[0009] Another object of the invention is to make electronic transaction information available to the user simultaneously with transaction.

[0010] A further object of the present invention is to allow a user to easily access and use transaction information sorted by institution and date.

[0011] Yet another object of one embodiment of the present invention is to provide an interactive record of transactions, which can interact with the institutional records when it is necessary to revisit transactions.

[0012] A further object of the present invention is to provide transaction records stored in a user-carried dongle, which records may be transferred to and merged with other accounting records of the user

[0013] An additional object of the present invention is to provide a system which allows the user to avoid carrying numerous "vendor cards" by having the electronic card information stored on a user carried electronic device, a dongle such as a PMD (Personal Memory Device), (UCIM) Universal Customer Interface Module or an ISIM (Issuer Specific Interface Module).

[0014] Still another object of the present invention is to provide a consumer subsystem which is entirely personal to a single consumer, with security activation built in, whether by PIN identification, thumbprint activation, biologically specific user input or the like.

[0015] Yet another object of the invention is to provide system wherein the institution may access membership information and credit information from a single source; minimizing transaction steps.

- [0016] Another object of the present invention is provide a method of creating and storing meta records of each transaction, with identical copies existing in the institutional memory and the user's device memory.
- [0017] A further object of the invention is to provide a system where transactions may be permitted to only go forward after each participant accepts the other's identification as valid.
- [0018] Briefly, one preferred embodiment of the present invention is a device, system and method for electronically providing transaction information to a consumer/user in a contemporaneous manner. Institutions having transaction information supply terminals (TIST) such as cash registers and ATMs will provide dataports (typically USB ports or wireless interface) on a transaction device, such as a cash register or ATM, into which a user may interface (insert) a personal memory device (PMD), such as memory stick, thumb drive or the like, to electronically receive and store data. At the end of each transaction the transaction details, keyed to the institution and date, will be transferred from the transaction device to the personal storage unit. The user may then transfer records periodically to a personal computer or similar device programmed to receive, store and manipulate the data for accounting and management purposes.
- [0019] The components of the overall system of the preferred embodiment are an institutional transaction device provided with an external, consumer accessible dataport, the transaction device being programmed to download receipt and other transaction data via the data port. The user will have a personal memory device (PMD) compatible with the dataport. The user mates the PMD with the dataport and, at the close of the transaction, a discreet data packet is downloaded to the PMD including all of the transaction details, and being keyed to the institution and the transaction date and time. The data packets can be downloaded from the PMD into the user's personal computing equipment and printed or displayed as necessary for review. Optimally, the user may have software available to receive the data packets and utilize these for detailed reporting, collation and manipulation into usable reports and categorizations.
- [0020] A deluxe version allows the institutional TIST to have limited two-way communication with an enhanced version of the PMD referred to as a Universal Consumer Interface Module (UCIM), exchanging recognition information, vendor membership information, credit and financial information and the like. The two-way capability is triggered only after security activation by the consumer, such as by use of a PIN or a biogenic key. The deluxe version permits high speed electronic communications during the transaction and facilitates rapid processing.

- [0021] A further embodiment of the invention involves a universal customer interface with a self authenticating UCIM referred to as a dongle which may be used either with onsite dataport or with wireless or internet communications for secure and rapid transactions. The dongle may be in the form of an Issuer Specific Interface Module (ISIM) which is uniquely associated with both an Issuer and a particular User.
- [0022] An advantage of the present invention is that it may be used to store the user's personal information, such as for vendor cards, ATM cards, credit cards and the like which may be directly accessed by the institutional transaction subsystem, thus eliminating the need for carrying multiple cards.
- [0023] Another advantage of the invention is that it can be provided with internal security such that an institution may only retrieve information matching its own code which has been previously downloaded into the PMD, UCIM or ISIM, such as receipts from prior transactions, vendor cards and the like.
- [0024] An additional advantage of the invention is that personal security may be built into the PMD, UCIM or ISIM such that only the intended user will be able to activate the dongle in use, with the personal security options including PIN activation and physical or biogenic activation, such as by thumbprint.
- [0025] A further advantage of the invention is that it helps save the environment by eliminating a significant source of waste for disposal, that being the numerous printed transaction receipts.
- [0026] Yet another advantage of the present inventive system is that user dongles may be customized by credit issuers, banks and the like and may be made personal to each user, so that only that user can activate certain feature.
- [0027] Still another advantage of the invention is that self-authenticating dongles can be utilized in merchant transactions which are very fast and which are much more secure than those using conventional debit cards, since only the authenticated user can make the dongle function.
- [0028] Another advantage of the present invention is that self-authenticating dongles using encrypted communications with credit authorization institutions can significantly improve the convenience and safety of online transactions.
- [0029] These and other objects and advantages of the present invention will become clear to those skilled in the art in view of the description of the best presently known mode of carrying out the invention and the industrial applicability of the preferred embodiment as described herein and as illustrated in the several figures of the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0030] Fig. 1 is a diagrammatical view of a Universal Customer Interface embodiment of the inventive system, particularly illustrating the components;
- [0031] Fig. 2. is a diagrammatical view of a Universal Customer Interface embodiment of the inventive system, particularly illustrating the connections and relationships among the components; and
- [0032] Fig. 3 is a diagrammatical view of the components of the UCI dongle of the inventive system.

BEST MODE FOR CARRYING OUT THE INVENTION

- [0033] The present invention is a system for carrying out paperless transactions **10** and is adapted for use in a commercial type transaction **11** between a consumer and an institution. The overall system is designated by the general reference character **10** and includes two component subsystems. An institutional subsystem **12** includes all of the components on the part of the institution (vendor, store, online merchant, online service provider, bank or the like) while a consumer subsystem **14** includes all of the components used by the consumer. Both subsystems **12** and **14** are necessary and work in combination for effective usage.
- [0034] A simplified system **16** is envisioned where the intention is to simply record and retrieve transaction data while avoiding the use of paper. This will involve merely recordation of generally non-sensitive transaction information and will not involve extensive security precautions. A deluxe system **18** is also envisioned which involves a great deal more personal and sensitive information and two-way communications, thus requiring additional security precautions. Both simplified system **16** and deluxe system **18** involve similar components and operations and they share the basic functions.
- [0035] In each case the institutional subsystem **12** will include a transaction device **20** such as a cash register, ATM or the like. The transaction device is ordinarily a transaction information supply terminal (TIST) **22** which is typically a moderately sophisticated data processing system programmed to interact with the consumer (and sometimes with institutional personnel, such as cashiers). The TIST **22** will be provided with consumer input structures **24** which may include a keypad, a card reader, bar code scanner, biological interface devices (such as fingerprint or thumbprint readers and , in embodiments envisioned

for the future, DNA comparison components), voice activated devices, or even direct interface with live personnel. The TIST 22 will also (at least in past embodiments) include a printer 26 for providing a transaction record (receipt or tally) 28 for delivery to the consumer at the end of the transaction. The transaction record 28 is useful for memorializing the transaction and for occasional use, such as when a return of an item is made to the institution or for the purposes of correcting a discrepancy. In the past, these transaction tallies 28 were usually discarded very quickly, thus adding to the volume of paper trash affecting the embodiment. In some instances, of course, the consumer would instead retain the paper tally 28 in a shoebox or the like for accounting and tax purposes.

[0036] A feature of the present invention 10 is that the institutional subsystem 12 is provided with a consumer accessible dataport 30. In technology which is current as of the writing of this patent application, the dataport 30 is envisioned to be a USB port 32, although numerous other types of dataports 30 are currently envisioned and many more will undoubtedly be utilized in the future. Envisioned varieties of dataports 30 include wireless interfaces such as RFI scanners, optical interfaces, ultrasound interfaces, and Bluetooth, all of which are capable of delivering and exchanging information between two components. The dataport 30 is adapted to interface with a personal memory device (PMD) 34 carried by, and personal to, the consumer.

[0037] The TIST 22 is provided with a printer interrupt 36 which will activate whenever a PMD 34 is engaged with the dataport 30. This will, unless overridden by input from the consumer or institutional personnel, cause the transaction report 28 to be delivered only to the PMD 34 and not to the printer 26. In this manner paper and ink are saved whenever a consumer uses a PMD with the system 10.

[0038] The transaction report 28 delivered from the TIST 22 to a PMD 34 is not the same as a printed receipt in all particulars. Instead, it is in the form of an electronic transaction record (ETR) 38. Each ETR 38 will include particular electronic coding to uniquely identify the particular transaction and tag the electronic packet in a way that it can be recognized, separated from and sorted in relation to other transactions. The coding will include an institutional ID 40 specifying the particular institution and location of the TIST 22. There will also be date and time coding 42 as part of a packet header. In addition, each individual transaction entry 44 in the transaction 11 (such as separate items purchased at a grocery store) may include an electronic item ID 46 such as a bar code or other inventory identifier associated with the item by the institution.

[0039] The ETR 38 is adapted to be printed out by the user in conjunction with other software available to the consumer, in the event that a paper record is needed for some purpose. In addition the ETR 38 is adapted to interface with recordkeeping software, such as personal financial accounting programs which may be used to parse and analyze the transactions. The PMD 34 is fully compatible with other machines having the same sort of dataport 30 (especially in the case of a USB port 32) and the consumer uses are virtually unlimited. Of course, it is also possible to recreate the ETR 38 for dealing with the particular institution, such as when returning merchandise. In the simplified system 16 embodiment, the institution may have an available processor 46 separate from the TIST 22 (such as at a Customer Service counter) which will also have a dataport 30, so the same effect as a paper receipt can be duplicated. In the deluxe system 18 embodiment, the TIST 22 itself may have two-way communication ability and the ETR 38, along with other information on the PMD 34 may (depending on the degree of access permitted by the associated software) be accessed by the TIST 22 for use.

[0040] The simplified embodiment 16 described above is sufficient for a primary purpose of the invention, that being the ability to minimize paper and ink expenditures resulting from commonplace transactions. This alone would be a great benefit to institutions and society as a whole. For such implementations the ordinary sort of commonly commercially available (relatively passive and inexpensive) PMD devices, commonly known as "thumb drives" or USB memory devices are entirely sufficient, since the only purposes are to provide memory storage for the ETR 38 and to activate the dataport communications. However, numerous other purposes may be accomplished by the deluxe system 18 embodiment, with enhanced software and greater two-way communication between the PMD 34 and the TIST 22. In such cases, a functionally enhanced PMD 34, referred to as a Universal Customer Interface Module (UCIM) 47 is utilized with enhanced memory and logic to facilitate interactive two-way communication with the TIST 22.

[0041] In the deluxe system embodiment 18 the TIST 22 is enabled to draw information from the UCIM 47 directly. Thus, the TIST 22 is provided with upload capacity 48. The upload features of the TIST 22 may be activated either by specific encoding in the particular packets or by consumer triggering using the consumer input 24 features. In either of these methods the institution may (depending on the particular software) be authorized and enabled to access some limited amount of personal data from the UCIM 47.

[0042] The consumer will be able, in the deluxe system embodiments 18, to store significant personal information on the UCIM 47. This will be carried in discreet packets corresponding to different types of data. Typical information will include personal ID information 50, vendor membership information 52, credit and financial information 54 and the like. The personal ID information 52 may include driver's license numbers, address and telephone and other specific information which may be necessary to transactions. Vendor membership information 52 will be the same that typically carried on cards specific to a particular vendor, such as purchasing clubs, discount cards and the like which are keyed to the store, health club or the like. By placing the vendor membership information 52 on the UCIM 47 the consumer save wallet or purse space and increases convenience. The credit/financial information 54 will be information typically carried on individual credit cards or bank ATM cards. As will be discussed in more detail hereinafter, the particular UCIM 47 utilized in some cases may be a Issuer Specific Interface Module (ISIM) 55 associated with a particular credit issuer of bank and carrying greater details particular to the accounts between the user and that issuer.

[0043] The personal ID information 50 will ordinarily not be particularly sensitive. Therefore, it is envisioned that special security encoding will not be necessary, as this will be the same sort of things ordinarily found on ID cards or the like used in verifying transactions. Accordingly, this will ordinarily be transparent to the TIST 22. However, it may be desirable to make this accessible only when manually triggered by the consumer, in order to protect privacy when desired.

[0044] The vendor membership information 52 will be semitransparent in most cases. That is, each item in the vendor info 52 will be specifically tagged with encoding particular to the vendor. That is, each store or institution will have particular coding corresponding to its own membership identifiers and the TIST 22 will be programmed to access only such information corresponding to the particular information. In this manner, the UCIM 47 will be inserted into the dataport 30 and the membership will be immediately recognized by the corresponding TIST 22, providing building access and discounts on purchases, or whatever other benefits are involved, all in a single step. The typical UCIM 47 will include multiple vendor membership packets corresponding to all of the particular groups to which the individual consumer subscribes. The information can be loaded on the UCIM 47 either directly from the institutional TIST 22 at time of sign-up or from the consumer's own computer. This feature may also be used for medical record cards and the like where additional patient specific information may be stored.

- [0045] The credit/financial information 54 is the most sensitive and will be specially encoded and protected from unauthorized upload to the particular TIST 22. It is envisioned that access to this information will be specifically triggered by the consumer using corresponding input. For example, if a consumer wishes to pay for purchases using a VISA card, a button on the consumer input 24 may be activated which allows access to credit/financial info 54 corresponding to VISA cards. If multiple such accounts are stored on the UCIM 47, a selection screen would be presented to allow the consumer to determine which VISA card was intended. Alternatively, the user may have a specific PIN or the like corresponding to each account and may enter this to permit the TIST 22 to access the corresponding information.
- [0046] For enhanced security and privacy, the UCIM 47 may be set such that it cannot be automatically activated and will be intensely personal to the particular consumer. Personal security protection 56 is provided to minimize the potential that the UCIM 47 could be stolen and used by another. One preferred form of personal security 56 is the use of a particular PIN 58 (Personal Identification Number) which the consumer must enter in order to unlock access to the UCIM 47 at all. A password is the alphanumeric equivalent of a PIN 58 and may be used in the same way if the interface is sufficiently sophisticated. Another preferred method would be a thumbprint reader 60 built into the PMD 34. The thumbprint reader 60 is keyed specifically to the personal owner of the PMD 34 and only the application of the correct thumbprint subsequent to insertion of the PMD 34 into the dataport 30 will "unlock" access to the contents of the PMD 34.
- [0047] The thumbprint reader 60 discussed above is only one type of biological identifier device 62 which may be utilized to guarantee personal security. Other existing technology which could be used include fingerprint readers, voice print comparators, retinal scan comparators and readers of embedded code circuits in the user's body (RFID devices). Future technology will no doubt include DNA scanners capable of analyzing and matching a particular user's DNA from a touch or a breath sample.
- [0048] The biological identifier device 62 may be part of the UCIM 47 or may be part of the TIST 22 or other part of the institutional subsystem 12. There are advantages to having the biological identifier device 62 be part of the UCIM 47 in that access to the information in the UCIM 47 is controlled completely by the user on a local basis. This facilitates use of the UCIM 47 remotely, such as over wireless or internet type connections, thus greatly expanding the types of transaction which may be handled using the system 10. For other

purposes, such as reduced manufacturing costs for the UCIM 47, the biological indemnification device 82 may be part of the institutional subsystem 12. Further, if flexibility for sharing use with a trusted friend or family member is important, it may be desirable to use the previously discussed PIN or password identification methods.

[0049] One envisioned commercial application of the system 10 involves the use of the Issuer Specific Interface Module (ISIM) 55. This special embodiment is referred to as the Universal Customer Interface 64 and is illustrated in the several figures of the drawing. Fig. 1 Shows the Universal Customer Interface 64 in terms of its various components. Fig. 2. illustrates the connections and relationships among the components and Fig. 3 shows the aspects of the preferred UCIM 47 (referred to as a “dongle”) utilized in this embodiment.

[0050] Three (in some ways four) of the components illustrated in Fig. 1 are common to all of the embodiments of the present invention. The Customer (user) 66 is a necessary element of the invention since it is the user who must be involved to create any of the transactions 11 envisioned. Similarly an institution 68 (either the Merchant 70 or the Bank 72 of Fig. 1) is necessary to interact with the User 66 in any transaction 11, be it a purchase (merchant 70) or a financial transaction affecting an account (Bank 72). In addition, a dongle 74 is part of all embodiments, whether it is simple PMD 34, and more complex UCIM 47 or a self authenticating ISIM 55 as required for the Universal Customer Interface embodiment 64.

[0051] The deluxe dongle 74 of Fig. 1 is intended to be self-authenticating by carrying all of the critical information in its memory component 76 (usually a chip) and its logic component 78 (often a separate chip). The dongle 74 has an interface component 80 (presently embodied as a USB interface) which allows the dongle 74 to interface whether directly with the institutional subsystem 12 when present at an institutional facility with a corresponding dataport or with a personal computer (PC) 82 or equivalent device (internet enabled cellular devices or Bluetooth devices, for example) having a compatible dataport for remote transactions, such as over the internet where the user 66 and institution 68 are spatially separated. It is particularly desirable for remote transactions for the dongle to be self-authenticating so that the triggering/activation does not require any involvement of the institutional subsystem 12 and none of the sensitive identification information ever reaches the institutional records. By accomplishing this, the security problems related to transmitting sensitive data in readable form are minimized or eliminated. With a self-authenticating dongle 74 transactions 11 can be accomplished without the need of the institution 68 ever “knowing” the user’s credit card number, expiration date or code, for example. It is noted that in long distance (internet) transactions, paper receipts 28 are rarely concurrently

generated. For these purposes, there is no printer interrupt 36 function required, unlike the case with point of sale or ATM transactions.

[0052] When the Universal Customer Interface 64 is utilized to engage in a credit transaction the Credit Card Issuer (Issuer) 84 becomes directly involved. Rather than having the institution 68 separately query the Issuer 84, a direct connection is created between the dongle 74 and the Issuer 84. The Issuer's system will recognize the input from the dongle and will, provided the dongle 74 has been unlocked (authenticated) by the user, will automatically recognize the specific user 66 as genuine and will process the transaction (assuming, of course, that a viable credit relationship obtains). In the event that a direct account withdrawal is desired from the user's bank to supply funds to an institution, the same sort of interaction will occur, with the Bank 72 filling the slot of the Issuer 84.

[0053] In order to be self authenticating, the dongle 74 must be provided with hardware and/or software to recognize user-unique authentication. Only when this is provided will the dongle 74 (via the logic component 78) unlock the sensitive information 54 contained in the memory component 76 so that remote or institutional access is permitted to such. The preferred approach to self-authentication is to provide a biological identifier device 62 as described above built into the dongle 74. This will allow unlocking only when the actual user 66 physically (or sonically) interacts with the dongle after the dongle has been plugged into (or otherwise interfaced) with the dataport. A less-preferred authentication may be accomplished by using a PIN 58 or password activation which can be input into the dongle 74 from a keypad associated with the PC 82 at which the user is physically present (either at a transaction-remote location, such as the user's home or at the TIST 22 for direct transactions). In either event, the special construction of the dongle 74 requires the involvement of a Dongle Manufacturer 86 to create the specially equipped dongle 74.

[0054] The connections and relationships among the components, illustrated in Fig. 2, are discussed in more detail below in the Industrial Applicability section.

[0055] The components of the UCI Dongle 74 are illustrated in Fig. 3. The interface component 80 is illustrated in this figure as a USB port. The memory component 76 is illustrated as a memory chip which stores the records created by the user 66 and the issuer 84 plus any ETR records 38 created during use. The types of data stored on the memory component will typically include Personal ID information 50, vendor member information 52 and credit/financial information 54 as well as encryption keys, and the biological identification device 62 pattern (biometric data) to be matched in order to activate the two way communication. The memory component 76 will also store the utility programs

necessary to the various functions. The logic component 78 is illustrated as including a processor chip and a stored operating system, as well as the utility programs stored on the memory component 76. In the embodiment illustrated, the biological identifier device 62 is a thumbprint reader 60.

[0056] It is envisioned that particular Credit Card Issuers 84 and/or Banks 72 may wish to incentivize the use of the inventive system 10 and instill particular customer loyalty in their own credit programs by issuing the Issuer Specific Interface Module (ISIM) 55 to customers. The ISIM 55 will be provided to a customer already preprogrammed with the personal credit financial information 54 specific to the user's account with the Issuer 84 and with utility programs specifically adapted to operate in conjunction with the Issuer's TIST 22. The ISIM will be likely to be emblazoned with the trademarks and logos of the Issuer 84. The ISIM 55 may or may not be adapted to permit storage of vendor member information 52 for vendors other than the issuer 84.

[0057] Numerous other variants and modifications of the paperless transaction trail system 10 of the present invention may be envisioned and implemented. The above discussed embodiments are for exemplary purposes only and the appended claims are to be interpreted as encompassing the true and full spirit and scope of the invention.

[0058] While various embodiments have been described above, it should be understood that they have been presented by way of example only, and not limitation.

INDUSTRIAL APPLICABILITY

[0059] The paperless transaction trail system 10 of the present invention is intended for use by consumers and institutions as an electronic means of recording transactions. Full implementation will require efforts by both groups, but such will result in highly significant savings in paper and printing materials and will drastically reduce the amount of waste contributed to the environment as a result of transactions.

[0060] A typical institution, for example the XYZ Grocery chain, implements the system 10 by installing a TIST 22 module into their cash register system, also providing a dataport 30 (USB port 32) accessible to the consumer at each station. Nothing prevents the cash register transaction from operating as before when the dataport 30 is not activated, but, when a consumer, such as Ms. Jane Doe, inserts a PMD 34 into the dataport 30 and activates access by inserting her PIN 58 or applying her thumbprint to the reader 60, multiple benefits automatically ensue.

[0061] Initially, the printer 26 is disabled for the transaction by the printer interrupt 36, although this may be overridden manually if desired. Next, the TIST 22 accesses the corresponding encoded vendor membership information 54 and recognizes that Jane Doe is a member of the XYZ Preferred Buyer's Club and is entitled to discounts on some items purchased. This allows the TIST 22 to recalculate pricing on the affected items and concurrently present the correct charges on the virtual receipt. At the time that payment is required Ms. Doe provides manual input to the consumer input structure 24 to select payment by VISA, which allows the TIST 22 to access the VISA information 54 on the PMD 34 and perform the customary credit check electronically with the issuing institution.

[0062] At the close of the transaction 11, the TIST downloads an ETR 38 to the PMD 34, with the ETR 38 including an institutional ID 40 and Date and Time coding 44 specific to the transaction 11. Further each item purchased will have a transaction item entry 44 in the ETR 38 which will adequately identify the item (e.g. a jar of pickles) as well as the price. In this case, the TIST 22 will also update Jane Doe's membership information 52 in the XYZ Club by updating the running tally of purchases made, indicating that she is eligible for a larger discount on the next transaction 11. Ms. Does disengages her PMD 34 from the dataport 30 and leaves with only her purchases, unburdened by a wasteful ½ meter long receipt.

[0063] Later in the day, Ms. Doe realizes that she purchased the wrong type of pickles and returns to XYZ in order to return or exchange the item. Jane Doe again plugs her PMD 34 into the dataport 30 and the ETR 38 is accessed by the TIST 22 (which can immediately recognize the Institutional ID 40 and date and time coding 42 corresponding to the particular transaction 11. The prior purchase is clearly acknowledged and the revised transaction is easily accomplished, with Jane Doe leaving XYZ quickly and happily.

[0064] At a time of her choosing, Jane Doe then connects her PMD 34 to her own personal computer and downloads the relevant ETRs 38 into her accounting program, which processes the information. In this case, Ms. Doe is entitled to a specific tax deduction for pickles and the transactions are duly noted for inclusion on her tax return. All is accomplished without paper.

[0065] The inventor refers to the Consumer subsystem 14 as a SHUBOX™ since it replaces the physical shoe box into which paper receipts and the like are typically stored for sorting and use when accounting is required. Since the SHUBOX 14 is convenient and easily storable, it saves a great deal of hassle for the user. The PMD 34 contents can be duplicated onto personal computer memory and, if needed, onto another PMD to protect against catastrophic events such as memory failure.

[0066] In the case of the Universal Customer Interface embodiment 64 the initial impetus is likely to come from the credit Issuer 84. The Issuer 84 will commission the manufacture of customized dongles 74 (emblazoned with Issuer's logo) from the Dongle Manufacturer 86. These are then provided with Issuer specific programming in logic component 78 for facilitating easy recognition and interface with the Issuer's TIST 22. The customized dongles 74 are then apportioned out to users 66 (either new customers of Issuer 84 or existing credit card holders). When apportioned to the User 66 the customized dongle 74 will already be provided with the customers specific account information and other identification information already in the Issuer's files. The User 66 will then activate the dongle 74 and provide the security input to facilitate unlocking the two way communication mode. For full security, it may be that this initial activation may take place at an Issuer monitored location or it may be performed by the user at the user's PC 82, with appropriate security safeguards such as password or security question input to open the dongle 74 for programming. In the embodiment discussed above, the dongle 74 is readied by the software and the user will place a thumb on the thumbprint reader 60 in order to record a reference pattern for comparison. This biological identifier is saved in the memory component and locked in "permanently". In this manner the dongle 74 is completely personalized to the user and can only be used by the particular person to whom it has been issued.

[0067] When the customer 66 engages in a point of sale transaction the dongle 74 functions as discussed above for most purposes. However, when it comes time for payment, the customer 66 will activate the dongle 74 by applying a thumbprint to the thumbprint reader 60 which will trigger the credit transaction. The TIST 22 associated with the merchant 70 will recognize the coded signal generated by the dongle and will initiate direct communication with the institutional subsystem 12 of the Issuer 84, which instantly recognizes the encrypted signal form the dongle 74 as identifying the authenticated user 66 and the account and contemporaneously authorizes the payment to the Merchant 70. This authorization and payment is accomplished without the Merchant's system ever having access to any of the credit/financial account information 54 or personal identification information 50 of the User 66. This credit transaction takes place with approximately equal or better speed than those of conventional debit card transactions, but with a much greater degree of security, since only the activated User 66 can use his or her dongle 74. The dongle 74 also records each transaction 11 with an ETR 38 stored in memory for later use, as discussed above.

[0068] When the User 66 wishes to undertake a remote transaction (such as over the internet) the dongle 74 is inserted into the USB dataport on the user's own PC 82 (or a similar device

at which the User 66 is physically present. The transaction is activated when the User 66 applies the thumbprint when the dongle 74 is powered (through the USB connection). This unlocks the communication and facilitates sending the encrypted authorization to the Issuer 84. As the only sensitive information Credit/Financial information 54 transmitted over the internet is the encrypted signal recognized by the Issuer, this transaction is much more secure as the internet Merchant 70 or service provider (such as an online role playing or gaming site) does not receive any of this information, only the authorization from the Issuer 84. Data errors involved in entering information are also prevented. Thus the transaction is more convenient, accurate and secure than present technology.

[0069] The convenience, positive environmental impact, and security advantages of the present invention are of great benefit to the consumer. Similarly, the printing material savings, electronic form of transaction data and convenience of transactions are of great benefit to the institutions.

[0070] For the above, and other, reasons, it is expected that the paperless transaction system 10 of the present invention will have widespread industrial applicability. Therefore, it is expected that the commercial utility of the present invention will be extensive and long lasting.

IN THE CLAIMS

While various embodiments have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of a preferred embodiment should not be limited by any of the above described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

What is claimed is:

- 1 1. A paperless transaction system for use in transactions between an institution and a
2 consumer, comprising:
3 an institutional subsystem having a processing unit and at a consumer accessible dataport;
4 and
5 a consumer subsystem including a user-carried memory device dongle personal to the
6 particular consumer, said dongle being adapted to interface with said dataport; wherein
7 transaction data specific to the transaction is downloaded to said dongle through said
8 dataport, as an alternative to a printed transaction record.
- 1 2. The paperless transaction system of claim 1, wherein
2 said consumer accessible dataport is a USB port.
- 1 3. The paperless transaction system of claim 1, wherein said consumer accessible dataport is
2 a wireless interface adapted to recognize and exchange data with said dongle.
- 1 4. The paperless transaction system of claim 1, wherein
2 said transaction data includes an encrypted transaction number assigned to the particular
3 transaction, said encrypted transaction number also being associated with transaction
4 records maintained by said institutional subsystem.

1 5. The paperless transaction system of claim 1,
2 engagement of said dongle with said consumer accessible dataport triggers a printer
3 interrupt to prevent printing of physical transaction records and directs transaction records in
4 electronic form to said dongle.

1 6. The paperless transaction system of claim 1,
2 said dongle is made user-specific so it will only operate with a particular user by
3 embedding personal security triggering therein, said personal security triggering permitting
4 access to information stored in said dongle only when the user provides a user-specific
5 identification trigger during said transaction which matches said embedded personal security
6 triggering.

1 7. The paperless transaction system of claim 6,
2 said user-specific identification trigger is selected from the group comprising: user-
3 provided data input in the form of a personal identification number input by said user; user-
4 provided data input in the form of a password input by said user; and a biological identifier
5 specific to said user; and further wherein
6 said biological identifier is selected from the group comprising: fingerprint, thumbprint,
7 voice recognition pattern, voice command, retinal scan, embedded RFID matching and DNA
8 sampling.

1 8. A consumer interface system for two way communication between a consumer and a
2 vendor/institution, comprising
3 a vendor/institution subsystem including at least one transaction information supply
4 terminal (TIST) having a data processor programmed with operational software and a interface
5 port accessible to the consumer; and
6 a universal consumer interface module (USIM) adapted to be personally carried by the
7 consumer, said USIM including a physical dongle having a memory component, a logic
8 component and a port component compatible with said interface port;
9 wherein engaging said port component with said interface port initiates a transaction
10 mode between said USIM and said TIST.

1 9. The consumer interface system of claim 8, wherein the initiation of said transaction mode
2 disables physical print components associated with said TIST such that no concurrent physical
3 record of said transaction is generated.

1 10. The consumer interface system of claim 8, wherein
2 said memory component is preprogrammed with user specific data which said logic
3 component delivers to said TIST when said transaction mode is initiated; and
4 said data processor programming associates said user specific data with existing records
5 of said vendor/institution and activates any user-specific transaction modifiers which apply to the
6 particular user.

1 11. The consumer interface system of claim 8, wherein
2 said USIM is specific to a particular credit issuer;
3 said memory component includes data specific to the user's account with said credit
4 issuer; and
5 said logic component interacts with said TIST to invoke a credit transaction specific to
6 said user and said credit issuer.

1 12. The consumer interface system of claim 11, and further including
2 a user-specific security identification trigger unique to said user such that only said user
3 may activate said transaction mode between said USIM and said TIST.

1 13. The consumer interface system of claim 12, wherein
2 said user-specific identification trigger is a personal identification number input by said
3 user.

1 14. The consumer interface system of claim 12, wherein
2 said user-specific identification trigger is a biological identifier specific to said user.

1 15. The consumer interface system of claim 13, wherein
2 said biological identifier is selected from the group comprising fingerprint, thumbprint,
3 voice recognition pattern, voice command, retinal scan, embedded RFID matching and DNA
4 sampling.

1 16. A system for providing a transaction interface between an institution in the form of a
2 vendor, service provider or credit provider and a consumer entity, comprising:
3 an institutional computing and data subsystem provided by the institution to control and
4 record a transaction, said institutional subsystem being partially accessible by the consumer
5 entity; and
6 a consumer subsystem personal to the consumer entity for accessing said institutional
7 subsystem and interchanging data during said transaction, said consumer subsystem including a
8 physical dongle having a memory component, a logic computing component and an interface
9 component.

1 17. The system for providing a transaction interface of claim 16, wherein
2 the accessibility of said institutional subsystem is accomplished over a remote network;
3 and
4 the consumer entity engages said interface component of said dongle with a consumer-
5 entity-controlled electronic communications device accessing said remote network.

1 18. The system for providing a transaction interface of claim 16, wherein
2 the accessibility of said institutional subsystem is accomplished by a point-of-transaction
3 dataport; and
4 the consumer entity engages said interface component of said dongle by placing said
5 dongle into interface position with said point-of-transaction dataport.

1 19. The system for providing a transaction interface of claim 16, wherein
2 said dongle provides access between said institutional subsystem and said memory
3 component only after being provided with an unlocking trigger by the consumer entity; said
4 unlocking trigger being selected from the group comprising: PIN number, password, fingerprint,

5 thumbprint, voice recognition pattern, voice command, retinal scan, embedded RFID matching
6 and DNA sampling.

1 20. The system for providing a transaction interface of claim 16, wherein
2 said dongle memory component includes consumer entity specific credit information
3 which may be utilized by said institutional subsystem to trigger a credit transaction without
4 further information provided by the consumer entity.

Universal Customer Interface

Components

Dongle Mfg.
Master system

Customer
Credit card account
and a PC with
Internet access

Credit Card
Issuer
Master system

1/3

SUBSTITUTE SHEET (RULE 26)

Merchant
Hardware:
Cash register mod.
Software:
Interface on C/R

Dongle
Memory Chip
Interface

USB

Fig. 1

Bank
Hardware:
(Existing)
Software:
Interface to System

Universal Customer Interface

Connections & Relationships

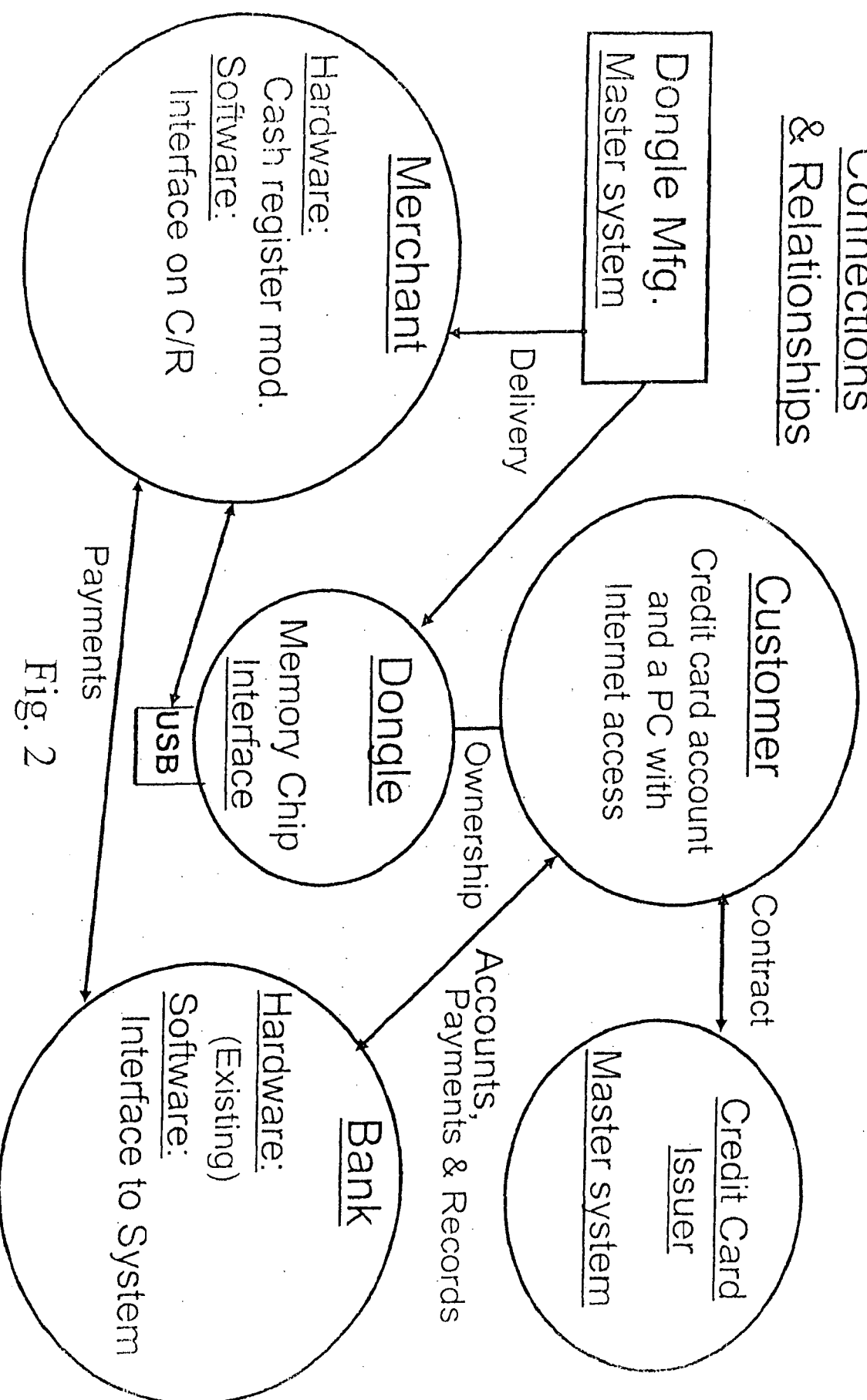


Fig. 2

UCI Dongle

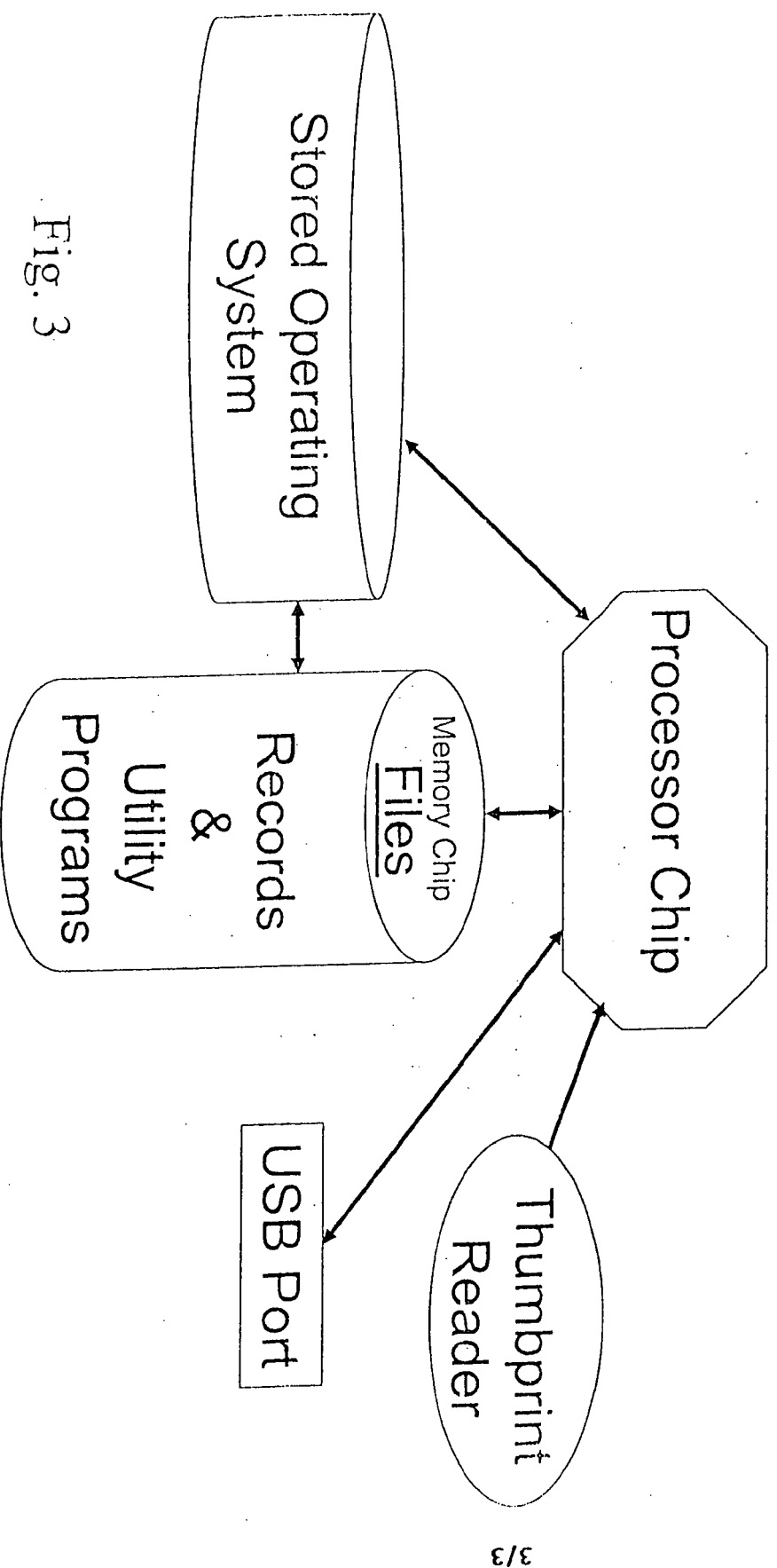


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 08/07921

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04K 1/00 (2008.04)

USPC - 705/55

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - H04K 1/00 (2008.04)

USPC - 705/55

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 902/40; 713/150; 705/17, 404; 709/217 (text search - see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PubWEST(USPT,PGPB,EPAB,JPAB); Google Scholar; Google Patents

Search Terms: dongle, dataport, USB, port, wireless, encrypted, transaction, number, PIN, fingerprint, thumbprint, voice, recognition, retinal, RFID, DNA, TIST, USIM, paperless, institution, consumer, prevent, block, disallow, printing

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 7,103,772 B2 (Jorgensen et al.) 05 September 2006 (05.09.2006), entire document especially col 5, ln 31-42, ln 46-50 and ln 51-67, col 6, ln 38-42, col 7, ln 49-50, col 9, ln 28-30 col 14, ln 6-25, col 15, ln 33-47 and ln 59-62, col 16, ln 60-66, col 17, ln 1-3, ln 10-16 and ln 23-30, col 31, ln 6-8	1-3, 6-8, 10-12 and 14-20 ----- 4-5, 9 and 13
Y	US 4,578,530 A (Zeidler) 25 March 1986 (25.03.1986), col 3, ln 17-30 and ln 61-63	4 and 13
Y	US 4,831,555 A (Sansone et al.) 16 May 1989 (16.05.1989), col 2, ln 17-18	5 and 9

☐ Further documents are listed in the continuation of Box C.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

11 October 2008 (11.10.2008)

Date of mailing of the international search report

29 OCT 2008

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774