

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
26 May 2005 (26.05.2005)

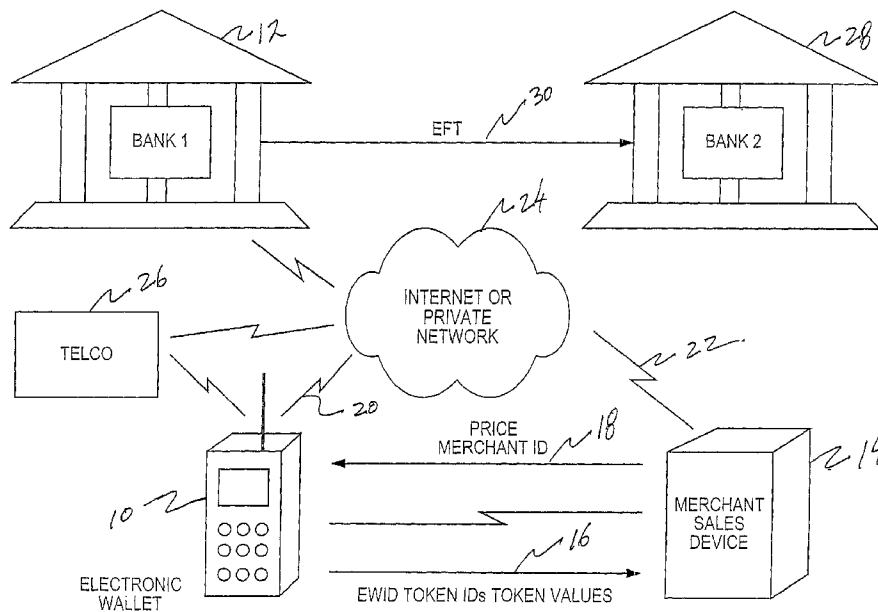
PCT

(10) International Publication Number
WO 2005/048082 A2

- (51) International Patent Classification⁷: **G06F**
- (21) International Application Number: PCT/US2004/037878
- (22) International Filing Date: 12 November 2004 (12.11.2004)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 60/519,693 12 November 2003 (12.11.2003) US
- (71) Applicant (for all designated States except US): **EXSENTRIK ENTERPRISES INC.** [US/US]; c/o Padell Nadell Fine Weinberger & Co., 156 West 56th Street, New York, NY 10019 (US).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **SOKOL, John, L.** [US/US]; 9839 Vernon Avenue, Montclair, CA 91763 (US).
- (74) Agent: **SCHWEITZER, Fritz, L, III**; Schweitzer Cornman Gross & Bondell LLP, 292 Madison Avenue-19th Floor, New York, NY 10017 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: ELECTRONIC COMMERCIAL TRANSACTION SYSTEM AND METHOD



(57) Abstract: A secure electronic commercial transaction system and method wherein electronic wallets and merchant sales devices exchange identification codes and identification codes and values of electronic monetary tokens and then simultaneously, independently communicate with a token issuing authority which compares the independently-transmitted identification codes of the devices and the identification codes and values of the electronic tokens and approves the transactions if all values match. The electronic wallet or the merchant sales device may communicate with the token authority through the other device via a secure funneling electronic communication protocol.

WO 2005/048082 A2



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.

ELECTRONIC COMMERCIAL TRANSACTION SYSTEM AND METHOD

Field of the Invention

[0001] The invention pertains to the field of commercial transaction systems and methods, and in particular to a secure wireless commercial transaction system and method suitable for public networks.

Brief Description of the Drawing

[0002] FIG. 1 is a schematic diagram of the method and system of the present invention.

Detailed Description of the Preferred Embodiments

[0003] Referring to FIG. 1, the invention is particularly suitable for consumer transactions wherein the consumer uses a portable electronic wallet device 10 (such as a cell phone, personal digital assistant, wristwatch, etc.) to authorize a payment to a merchant.

[0004] In the method, each electronic wallet 10 has a unique electronic wallet identification number (EWID). An issuing bank 12 acts as a token issuing authority and issues electronic monetary tokens to the electronic wallet 10, where each token has a fixed value that represents an amount of currency. Each token is assigned a unique token identification number (token ID), which is preferably a very large number (e.g., 1024 bits). Token IDs may be non-sequential to improve security. The token ID may also include an issuer identification code (Issuer ID) to identify the issuing bank (such as an ABA routing number, or the like), and a checksum value to check the validity of the token ID, issuer ID and/or token value.

[0005] The fixed value of each token may be one of \$0.01, \$0.02, \$0.04, \$0.08, \$0.16, \$0.32, \$0.64, \$1.28, \$2.56, etc., up to some predetermined maximum currency value. In other words, the value of each token is fixed at \$0.01 multiplied by 2 to the Nth power, where N is a whole number from 0 to some predetermined maximum value. Providing tokens in these binary, exponential multiples (i.e., 1, 2, 4, 8, 16, 32, etc.) of a minimum currency value (i.e., \$0.01) optimizes the "flow" of tokens. That is, if a user device has one

of every token up to a maximum token value, the user device will be able to redeem an exact amount for any purchase price up to the sum of all of the tokens. However, other denominations are also suitable, such as \$0.01, \$0.05, \$0.10, \$0.50, \$1.00, \$5, \$10, \$20, \$50, \$100, like current paper and coin currency.

[0006] Tokens are purchased by consumers by transferring cash or debt to the issuing bank 12. The IDs and values of purchased tokens are loaded into the consumer's electronic wallet 10. The issuing bank 12 compiles a database of issued tokens, which includes the token IDs, the values of the tokens, and the IDs of the electronic wallets 10 to which the tokens were issued.

[0007] During a transaction, there is an electronic communication 16, 18 between the electronic wallet 10 of the consumer and a merchant sales device 14 (such as a vending machine, kiosk, point-of-purchase system, or the like). There is also an electronic communication 20 between the electronic wallet 10 and the issuing bank 12, and an electronic communication 22 between the merchant sales device 14 and the issuing bank 12.

[0008] At the beginning of the transaction, the electronic wallet 10 receives a purchase price from the user as transmitted by the merchant sales device 14. The electronic wallet 10 then determines if it contains sufficient tokens to satisfy the purchase price. If enough tokens are present and the consumer authorizes the purchase, the consumer or, preferably, the electronic wallet 10 determines which of the tokens should be tendered to pay for the product or service. The token ID(s) and value(s) of the tokens selected to be tendered, and the ID of the electronic wallet 10 are then transmitted to the merchant sales device 14. Preferably the communication between the consumer's electronic wallet 10 and the merchant sales device 14 is wireless, for example, via the IRFM Infra-Red Financial Messaging standard, which uses the Infrared Data Association (IrDA) transmission standard.

[0009] In the next step of the transaction, the merchant sales device 14 and the electronic wallet 10 communicate independently with the bank 12 that issued the tokens. In each case, the token ID(s) and value(s), the electronic wallet ID and preferably the merchant sales device ID are transmitted to the issuing bank 12. If the information received from the merchant sales device 14 matches that from the electronic wallet 10, and if the tendered token ID(s) and values and the electronic wallet ID match the database records of valid

tokens at the issuing bank 12, then the issuing bank 12 responds separately to the merchant sales device 14 and the electronic wallet 10 validating the transaction. In addition, the issuing bank 12 marks the used tokens in the valid token database as being redeemed.

[0010] Preferably, the communication with the issuing bank 12 is, at least partially, via the public Internet 24. For example, the merchant sales device 14 may communicate with the issuing bank 12 via solely the public Internet 24, and the electronic wallet 10 of the consumer may communicate with the issuing bank 12 via the cellular phone network 26, as a first segment, and then the public Internet 24, as a second segment. While the public Internet 24 is a particularly suitable network, private networks are also suitable.

[0011] Upon receipt of the validation response from the issuing bank 12, the electronic wallet 10 removes the used tokens from its database (or marks them as used) and the merchant sales device 14 authorizes the release of the product or service. Immediately thereafter, or at some future time, cash or a credit equal to the purchase price is transferred from the issuing bank 12 to a merchant bank 28 via any suitable means, such as Electronic Funds Transfer (EFT) 30.

[0012] In the case where the consumer's electronic wallet 10 does not contain a combination of tokens that would produce the exact purchase price, the electronic wallet 10 may overpay for a product or service. The merchant sales device 14 and the electronic wallet 10 would then both transmit the purchase price to the issuing bank 12, in addition to the other information described above. Upon validating the transaction, the issuing bank 12 will pay/credit the merchant with the purchase price and will refund/credit the consumer with the overpayment. Preferably, the issuing bank 12 will refund the overpayment to the consumer by issuing new token(s) to the consumer's electronic wallet 10, which can be effected during the validation communication between the issuing bank 12 and the electronic wallet 10 or at a later time.

[0013] For a transaction to be secure, both the electronic wallet 10 and the merchant sales device 14 must communicate with the issuing bank 12 at the time of the transaction. Insecure transactions can occur if the merchant sales device 14 communicates with the issuing bank 12 after releasing the goods or service to the buyer. However, this transaction will be unsecured and at the risk of the seller. To reduce the risk of such "off-

line” transactions, each electronic wallet 10 may include a visible hologram containing all or part of the electronic wallet ID which can be verified by a human operator or a machine.

[0014] The merchant sales device 14 or the electronic wallet 10 may communicate with the issuing bank 12 through one another if necessary. This may be necessary, for example, if the merchant sales device 14 is a vending machine without a connection to the public Internet 24. In this case, the electronic wallet 10 could act as a router connecting the merchant sales device 14 with the issuing bank 12. The communication between the merchant sales device 14 and the issuing bank 12 would be through a secure encrypted tunnel using SSH or SSL, or a similar protocol, where the issuing bank 12 and the merchant sales device 14 have previously exchanged encryption keys unknown to the electronic wallet 10 or consumer. Thus, the electronic wallet 10 could not understand or imitate the communication between the merchant sales device 14 and the issuing bank 12. Where only the merchant sales device 14 is able to connect to the issuing bank 12, the electronic wallet 10 could communicate through the merchant sales device 14 in a similar manner.

What is claimed:

1. A method of conducting electronic commercial transactions, comprising:
 - providing a portable electronic wallet having a transceiver and a memory and having a unique identification code and a plurality of electronic monetary tokens stored in said memory;
 - each electronic monetary token representing a fixed value of currency and including a unique identification code and a value;
 - providing a merchant sales device having a transceiver and a memory and having a unique identification code stored in said memory;
 - providing a token issuing authority having a database containing records of said electronic monetary tokens stored in said memory of said electronic wallet, said electronic monetary tokens being associated to said identification code of said electronic wallet in said database,
 - said token issuing authority receiving a first electronic communication from said electronic wallet including said identification code of said electronic wallet, an identification code of at least one tendered electronic monetary token, a value of said tendered electronic monetary token and said identification code of said merchant sales device;
 - said token issuing authority receiving a second electronic communication from said merchant sales device including said identification code of said electronic wallet, said identification code of said tendered electronic monetary token, said value of said tendered electronic monetary token and said identification code of said merchant sales device;
 - said token issuing authority confirming said first and second electronic communications by comparing identification codes of said electronic wallet, said merchant sales device and said tendered electronic monetary token, and comparing said value of said tendered electronic monetary token, as received in said first and second electronic communications;
 - said token issuing authority validating said tendered electronic monetary token by comparing said identification code of said

electronic wallet and said identification code and said value of said tendered electronic monetary token to said records in said database; and

- 5
- said token issuing authority sending a transaction approval message to said merchant sales device if both said step of confirming said first and second electronic communications and said step of validating said tendered electronic monetary token result in a match.

2. A method as in claim 1, further comprising:

- 10
- said merchant sales device transmitting a purchase price to said electronic wallet;
 - said electronic wallet transmitting said identification code of said electronic wallet and said value of said tendered electronic monetary token to said merchant sales device.

15

3. A method as in claim 1, further comprising:

- one of said merchant sales device and said electronic wallet communicates with said token issuing authority through another one of said merchant sales device or electronic wallet via a secure
- 20
- electronic communication protocol.

FIG. 1

