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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 September 2002 (12.09.2002)

PCT

(10) International Publication Number
WO 02/071177 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/SG01/00024

(22) International Filing Date: 3 March 2001 (03.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **MONEYHIVE.COM PTE LTD** [SG/SG]; 11 Unity Street, Robertson Walk #02-13, Singapore 237995 (SG).

(71) Applicants and
(72) Inventors: **CHIA, Song, Chim, Jeffrey** [SG/SG]; Blk 110, #12-616 Potong Pasir Ave 1, Singapore 350110 (SG). **CHAN, Ying, Yip** [SG/SG]; Blk 140 Tiong Bahru Road #04-1086, Singapore 150140 (SG). **WONG, Ohn, Chee** [SG/SG]; Blk 557, Ang Mo Kio Ave 10, #02-1892, Singapore 560557 (SG). **YAP, Boom, Leong** [SG/SG]; Blk 9A Ghim Moh Rd, #09-148, Singapore 271009 (SG).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG)*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG)*

— *of inventorship (Rule 4.17(iv)) for US only*

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 02/071177 A2

(54) **Title:** METHOD AND SYSTEM FOR SUBSTANTIALLY SECURE ELECTRONIC TRANSACTIONS

(57) **Abstract:** A method and system of performing substantially secure transactions in the context of a remote commercial transaction via electronic communication, such as over the Internet. When in the following description reference is made to credit cards, it must be understood that this is intended to cover any kind of credit card, debit card, credit or debit account, savings or checking account, smart card or the like. The customer is prompted to enter his account name and PIN by using a data entry mean such as a graphical keyboard at an electronic device. Values of the graphical keys are randomly generated and delivered as a definition file from another electronic device along a secure channel to the customer's first electronic device. The corresponding data in the definition file, instead of the actual authentication data, are communicated over the network when the customer enters the authentication information. Once authenticated, the customer enters only a subset of the credit card account number to which the order is to be charged. Only this subset is transmitted over the network to the second device. Another subset of the credit cart account number is pre-stored with a trusted party, such as the merchant, a bank, credit card company, certificate authority, payment service provider or like. The two subsets are combined and transmitted to existing payment clearing networks for processing.

Method and System for Substantially Secure Electronic Transactions

Description

TECHNICAL FIELD

The present invention generally relates to a method of secure transaction via electronic communication, and more particularly, to a method of authentication and to a method for communicating user account information.

BACKGROUND ART

When in the following description reference is made to credit cards, it must be understood that this is intended to cover any kind of credit card, debit card, credit or debit account, savings or checking account, smart card or the like.

Online shopping represents an increasing part of the economy. The growth in its popularity can in part be explained because consumers have learned that goods purchased online are often much less expensive than if purchased through a normal retail store. In addition, because a customer can shop without leaving the comfort of home or office, placing an order for merchandise online makes much more efficient use of the customer's time.

A credit card facilitates making purchases over the network. However, users are justifiably concerned about placing orders for merchandise on networks such as the Internet, for example via E-mail, because of the lack of secure communications. Security on public networks at the present time is virtually non-existent, making it relatively easy for an unauthorized third party to gain access to credit card data transmitted over the network. Access from public terminals also exposes the customer to keylogging programs that can capture the credit card data. Once a dishonest person has the credit card number, thousands of dollars can be improperly

charged to the customer's credit card account.

One solution to this problem is for the customer to enter, for delivery over the network, an order that does not include the customer's credit card number. To complete the order, the customer must then call the merchant on an 800-telephone number, for example, to provide the credit card number. However, this method does not enable the credit card data to be readily associated and entered with the order previously placed by the customer. Errors in the order can easily arise. For example, the customer's credit card number can be assigned to the wrong order. In addition, there is usually a considerable delay to further inconvenience the customer while a clerk asks the customer other questions that will help to ensure the correct match between an order that was previously transmitted and the customer's credit card number given over the phone.

An approach as disclosed by the US Pat. 5,727,163 to Bezos et al requires an initial submission of a portion of the credit card data over the non-secure network from a local computer. The message with the portion of the credit card data is received at a remote location coupled to the non-secure network and is added to a database. A telephone call is placed to the remote location to finalize the message by entering complete credit card data. The message is then matched with the complete credit card data by comparing the portion of the credit card data that was included in the message with a corresponding portion of the complete credit card data that was entered over the telephone. The complete credit card data is thus matched with and entered into the message in the database to finalize the message. However, this approach is troublesome, as the customer has to make a subsequent phone call. If the customer has only a fixed home line that is being used for the online connection, he has to hang up and call to complete the transaction. This approach is obviously not suitable for purchases of digital content.

Another approach to solving this problem is to encrypt the credit card information included in an order placed on a public network. Using the encrypted credit card data, an order can be completed in a single transaction. However, virtually all of the

encryption schemes thus far developed for protecting such sensitive data have drawbacks. For example, most encryption schemes require the use of an encryption key that is known only to the party encrypting information and to the intended recipient of the information who will decrypt it. The secure distribution and safeguard of such encryption keys adds too much complexity to network shopping transactions and will likely not be readily accepted by customers. While it is possible to embed an encryption key in an application designed to take an order and transmit it over the network, the embedded encryption key can be discovered by others who may then misuse it. Even public key encryption systems require use of a "private" key that should not be disclosed to others. In addition, and perhaps more importantly, the software required for any encryption system must be distributed to prospective customers before the system can be used to transfer credit card data when a customer places an order. The widespread dissemination of such software will likely not occur for some time. In addition, this approach restricts the customer to the personal terminals where such software is installed. Terminals belonging to another person but with the software is useless too as the software is usually personalized upon installation.

A new method for ordering goods over a network is needed that. The present invention provides a system that (1) enables a customer to place an order without concern that others may illicitly gain access to the customer's credit card information, (2) relieve burden on the second (or trusted) party that others may illicitly gain access to their customer's full credit card information, (3) reveals no sensitive information to an observer and (4) reveals no information to someone posing as a customer. The present invention represents a workable solution to this problem that is relatively efficient and foolproof.

DISCLOSURE OF INVENTION

In accordance with the present invention, a method is defined for performing secure transactions in the context of a remote commercial transaction via electronic communication, such as over the Internet. When in the following description

reference is made to credit cards, it must be understood that this is intended to cover any kind of credit card, debit card, credit or debit account, savings or checking account, smart card or the like. The customer is prompted to enter his account name and PIN by using data entry means such as a graphical keyboard at an electronic device. Values of the graphical keys are randomly generated and delivered as a definition file from another electronic device along a secure channel to the customer's first electronic device. The corresponding data in the definition file, instead of the actual authentication data, are communicated over the network when the customer enters the authentication information. Once authenticated, the customer enters only a subset of the credit card account number to which the order is to be charged. Only this subset is transmitted over the network to the second device. Another subset of the credit card account number is pre-stored with a trusted party, such as the merchant, a bank, credit card company, certificate authority, payment service provider or like. The two subsets are combined and transmitted to existing payment clearing networks for processing.

By relieving the trusted party of storing the full credit card data, it prevents hacker attacks on its system, as the pre-stored subset of credit card data is useless to the hackers. In the preferred embodiment of the system, databases storing authentication and partial credit card data are separated and their access are controlled and logged.

Using the data entry means such as a graphical keyboard and its random values in the definition file, it prevents any capturing of authentication and credit card information, either at the customer's terminal or over the network. Hence, this system offers high degree of security to the customer even when accessing from a public terminal.

The present invention also protects the merchant and customer from the misuse of the customer's credit card by third parties. All credit card payments are verified against the pre-stored subsets of credit card data, hence unauthorized use of credit card is prevented.

BRIEF DESCRIPTION OF DRAWINGS

The foregoing aspects and many of the attendant advantages of this invention will become more readily appreciated as the same becomes better understood by reference to the following detailed description, when taken in conjunction with the accompanying drawings, wherein:

It should be understood that the following applications are by way of example, and should not be taken as limiting the scope of the invention.

Figure 1 is a schematic representation of a flow chart showing various steps involved in the performance of the system and method of the present invention for substantially secure transactions;
Figure 2 is a graphical representation of a process showing various steps involved in the performance of the system and method of the present invention for substantially securely communicating user information over a network between a first electronic device and a second electronic device during a session.
Figure 3 is a graphical representation of a process showing various steps involved in the performance of the system and method of the present invention for substantially securely verifying third-party information over a network between a first electronic device and a second electronic device during one of a transaction session.

Like reference numerals refer to like parts throughout the several views of diagrams.

MODE(S) FOR CARRYING OUT THE INVENTION

As shown in the accompanying Figures, the present invention is directed towards a system and method for accomplishing substantially secure transactions. For the purpose of illustration a credit card transaction is illustrated. It must be understood that this is intended to cover any kind of credit card, debit card, credit or debit account, savings or checking account, smart card or the like.

More specifically and with reference to Figure 1 the system as well as an attendant method is preferably instigated by the customer viewing a product, identifying a desired amount for a transaction as at 10, by an electronic device 1. Customer contact a custodial authorizing entity as at 12 by sending an activation request, such as clicking on a "Pay" button on the merchant site, from the electronic device 1 of customer to the electronic device 2 of the custodial authorizing entity. A custodial authorizing entity may herein be defined as comprising that entity or institution which has or has been designated by the entity which has custodial responsibility for the financial data and security of a given credit card account of a customer. The custodial authorizing entity is one of a merchant, a bank, a credit card company, a certificate authority, a payment service provider, and the like, receives the activation request and authenticates that the request is from a trusted source. The authentication includes checking of IP address of the origin of activation request and the like. Such authentication is known to those skilled in the art.

A new session is then created by the electronic device of the custodial authorizing entity at 16. The new session is given a unique Session Identifier. A set of random values corresponding to the letters (A-Z) in the alphabet and the digits (0-9) is also created at 16. Preferably, the letters should consist of both sets of lowercase and uppercase letters. It should also be noted that "pseudo-random" numbers, as this term is commonly used in the art to apply, for example, to time-based or list-based number generating systems, may be used in place of random numbers in the system of the present invention.

The random values are assigned accordingly to their graphical counterparts for the letters and digits. This can be achieved by tagging the random values to the corresponding graphical keys in the definition file belonging to the particular session. The icons or pictures for the alphabets and digits (0-9) can be in any of the commonly supported graphical formats, such as GIF, JPEG and PNG. These graphical letters and digits make up the graphical keyboard. Preferably, file names of the icons or pictures should be randomly generated too. Arrangement of the letters and digits may be varied regularly to enhance security.

A Session Database stores a complete set of information required for that session at the electronic device 2 of the custodial authorizing entity at 18. The information may or may not be encrypted when it is stored in the database.

The Session Identifier, graphical keyboard and other transaction information are delivered back as a definition file to the electronic device 1 of the customer over a secure channel such as SSL at 20. The definition file can take the form of a new browser window, the same browser window, a standalone Java applet, a Java applet embedded into a browser window or a browser plugin such as Flash SWF files. In the preferred embodiment of the system, a new browser window with an embedded Java applet is used.

A graphical keyboard is displayed on the electronic device 1 of the customer at 22. The customer then uses the graphical keyboard to enter the authentication data, instead of the physical keyboard. This prevents any key-logging software from capturing the authentication data, as it is impossible to capture. To further improve security, the screen location where the graphical keyboard appears or the arrangement of each key is changed from time to time to prevent others from "guessing" by observing the positions of the pointer or cursor.

Authentication data is transmitted over the network using a secure channel from electronic device 1 of the customer to the electronic device 2 of the custodial authorizing entity at 24. The present invention builds on security of existing network security protocols by sending only the session identifier and the random values of the keys returned by the customer. In the remotest chance of a hacker being able to intercept the messages, the information is useless in obtaining the actual values of the customer's input. It should also be noted that the use of screen coordinates may be used in place of random values in the system of the present invention.

When the custodial authorizing entity receives the authentication data, it retrieves from the Session Database, with reference to the Session Identifier, the actual values

of the customer's input at 26. The actual values are then compared with the previous knowledge of the customer's authentication information stored on an Authentication Database at electronic device 2 of the custodial authorizing entity at 28. This database can to be encrypted for added security.

Once the correct customer authentication is performed at 30, the custodial authorizing entity transmit verification correct to customer of electronic device 1 to get customer to enter the credit card information using the graphical keyboard at 32.

Customer credit information is transmitted over the network using a secure channel from electronic device 1 of the customer to the electronic device 2 of the custodial authorizing entity at 34.

Custodial authorizing entity may perform validation of customer credit number before approving transaction at 36.

Referring to Figure 2, an illustrated procedure shows how a registered customer is protected against unauthorised use of his credit card information by the merchant or any third party during electronic transactions. Such transactions include for example: purchasing goods or services by transferring funds (paying) to a merchant's financial account; or transferring funds between a person's personal accounts, including credit card, debit or stored-value and bank (saving or checking) accounts. Use of the procedure for the above transactions allows a customer to execute any electronic transaction from anywhere safely.

After being authenticated by the trusted party, the customer can choose to pay from any pre-registered credit card, savings, checking, prepaid or debit account. The customer then enters a subset of the credit card, savings, checking, prepaid or debit account number depending on the payment choices (Step 1). The graphical keyboard at 38 is used. In the remotest chance of a hacker being able to intercept the messages, the information is useless as only partial numbers are transmitted. Furthermore, the actual values transmitted are coded as random values.

The trusted party at 40 stores subsets of the customer's account number(s) in an Account Database. This database can to be encrypted for added security. A pre-stored set of the selected account number is retrieved from the Account Database and combined with the actual values of the customer's input (Step 2). The combined values and relevant information are joined to form a Transaction Message.

The Transaction Message (TM) is encrypted and sent over secure connections to existing banking networks for processing. The TM can be sent by the trusted party directly to the banking network at 42 or indirectly to the merchant who re-transmits it to the banking network as is known to those skilled in the art.

Referring to FIG. 3, an illustrated procedure shows how a registered customer and merchant are protected against fraudulent use of the customer's credit card by third party. Such transactions could include for example: purchasing a good or service by transferring funds (paying) to a second party's financial account; or transferring funds between a person's credit accounts, from credit to debit or stored-value accounts, to, from, or between bank (saving or checking) accounts.

This procedure is carried out by the customer at 44 first registering with the trusted party at 46 (Step 1). The trusted party, such as the merchant, a bank, credit card company, certificate authority, payment service provider or like, receives the registration and verifies that it is legitimate (Step 2).

The trusted party stores a subset of the customer's account data (Step 3). All subsequent transactions by non-registered customers are verified against the database of pre-stored account data (Step 4). When a non-registered customer at 48 enters information for purchases, the information is compared to the database of pre-stored account data that belong to the registered customers. This is performed by the trusted party at 50. If there is a match, the non-registered customer at 52 is asked to either log in or change the account information used for payment (Step 5) because a registered customer's data is being used without authorisation.

The present invention, therefore, prevents any fraudulent use of the registered customer's account by third party. However, the effectiveness of this system depends on the number of accounts that are pre-stored at the trusted party.

Claims

The invention in which an exclusive right is claimed is defined by the following:

1. A method of substantially securely transferring data over a network between a first electronic device and a second electronic device during a session, the method characterized by:

   (a) Transferring by the first electronic device to the second electronic device a definition file for association with a data entry means of the second electronic device;
   (b) Capturing user input by the data entry means; and
   (c) Transferring data in the definition file corresponding to the user input by the second electronic device to the first electronic device.

2. A method according to Claim 1, wherein the data entry means is one of a graphical keyboard and a numerical keypad that includes a plurality of keys.

3. A method according to Claim 2, wherein the data in the definition file includes one of values corresponding to the plurality of keys, screen coordinates corresponding to the display location of the data entry means, a session identifier, and transaction information.

4. A method according to Claim 3, wherein the values are different for each session.

5. A method according to Claim 1, wherein the data in the definition file is one of a randomly generated, a time-based generated, and a list-based generated and kept by the first electronic device.

6. A method according to Claim 1, wherein the definition file is one of a browser window, a standalone Java applet, a Java applet embedded into a

browser window, a browser plugin, a Flash SWF file, and a graphics bitmap file.

7. A method according to Claim 1, wherein the user input is one of a user password, a user access code, a credit card number, a prepaid account number, a debit account number, a bank account number, and a telephone calling card number.

8. A method according to Claim 1, wherein the user input is a partial one of a user password, a user access code, a credit card number, a prepaid account number, a debit account number, a bank account number, and a telephone card number.

9. A method according to Claim 1, wherein the electronic device is one of a personal computer, a computer main frame, a computer server, a computer system, a touch screen information kiosk, a vending machine, a web-enable television, a digital television, a mobile phone and a PDA.

10. A method according to Claim 1, wherein the network is one of a secure network, the Internet, a PSTN network, a mobile network and a wireless local network.

11. A method according to Claim 1, wherein the session is one of a registration session, a authentication session, a transaction session and a data entry session.

12. A method according to Claim 1, wherein the data entry means includes a graphical keyboard having a plurality of keys.

13. A method according to Claim 11, wherein the graphical keyboard is transferred from the first party to the second party.

14. A method according to Claim 12, wherein the keys are arranged according to a pattern.

15. A system for substantially secure data transfer over a network, the system characterized by:

(a) a first electronic device coupleable to the network; and
(b) a second electronic device coupleable to the network;

wherein in use a definition file for association with a data entry means of the second electronic device is transferable from the first electronic device to the second device so that user input can be captured by the data entry means and data in the definition file corresponding to the user input is transferable by the second electronic device to the first electronic device.

16. A program storage device readable by a processor, tangibly embodying a program of instructions, executable by the processor to perform a method for substantially securely transferring data over a network between a first electronic device and a second electronic device during a session, the method characterized by:

(a) Transferring by the first electronic device to the second electronic device a definition file for association with a data entry means of the second electronic device;
(b) Capturing user input by the data entry means; and
(c) Transferring data in the definition file corresponding to the user input by the second electronic device to the first electronic device.

17. A method of substantially securely communicating user information over a network between a first electronic device and a second electronic device during a session, the method characterized by:

(a) Transferring by the second electronic device to the first electronic device a first partial of a user information;

(b) Capturing the partial user information by the first electronic device from the second electronic device;

(c) Retrieving a second of a partial user information from the first electronic storage media, and

(d) Combining the first and the second partial user information together to obtain the complete user information.

18. A method of according to Claim 17, wherein the user information is a one of a user password, a user access code, a credit card number, a prepaid account number, a debit account number, a bank account number, and a telephone calling card number.

19. A method of according to Claim 17, wherein the storage media is a one of a computer hard disk, a CDROM and a ROM.

20. A method of substantially securely verifying user information over a network between a first electronic device and a second electronic device during one of a registration and a transaction session, the method comprising:

(a) Registering user information of the first electronic device with the second electronic device during the registration session.

(b) Pre-storing the full user information of a first electronic device in the second electronic device storage media during the registration.

(c) Transferring by the first electronic device to the second electronic device a first partial of a user information during the transaction session;

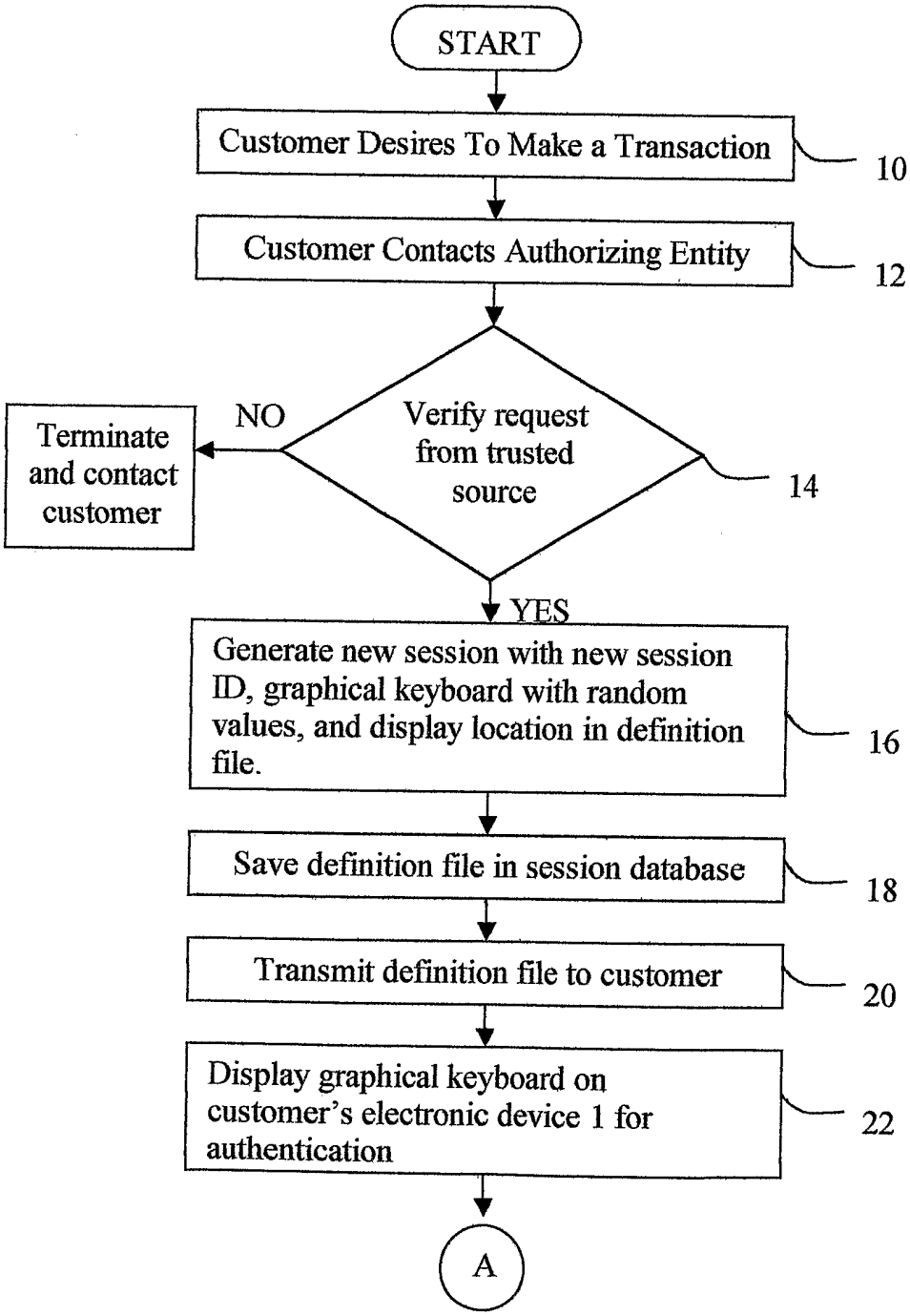
(d) Capturing the partial user information by the second electronic device from the first electronic device during the transaction session;

(e) Retrieving a second of a partial user information from the second electronic storage media during the transaction; and.

(f) Comparing the partial user information with one of a full user information, and a partial user information of previous knowledge in the second electronic storage media.

Drawings

Figure 1: Secure Authentication for Electronic Transactions



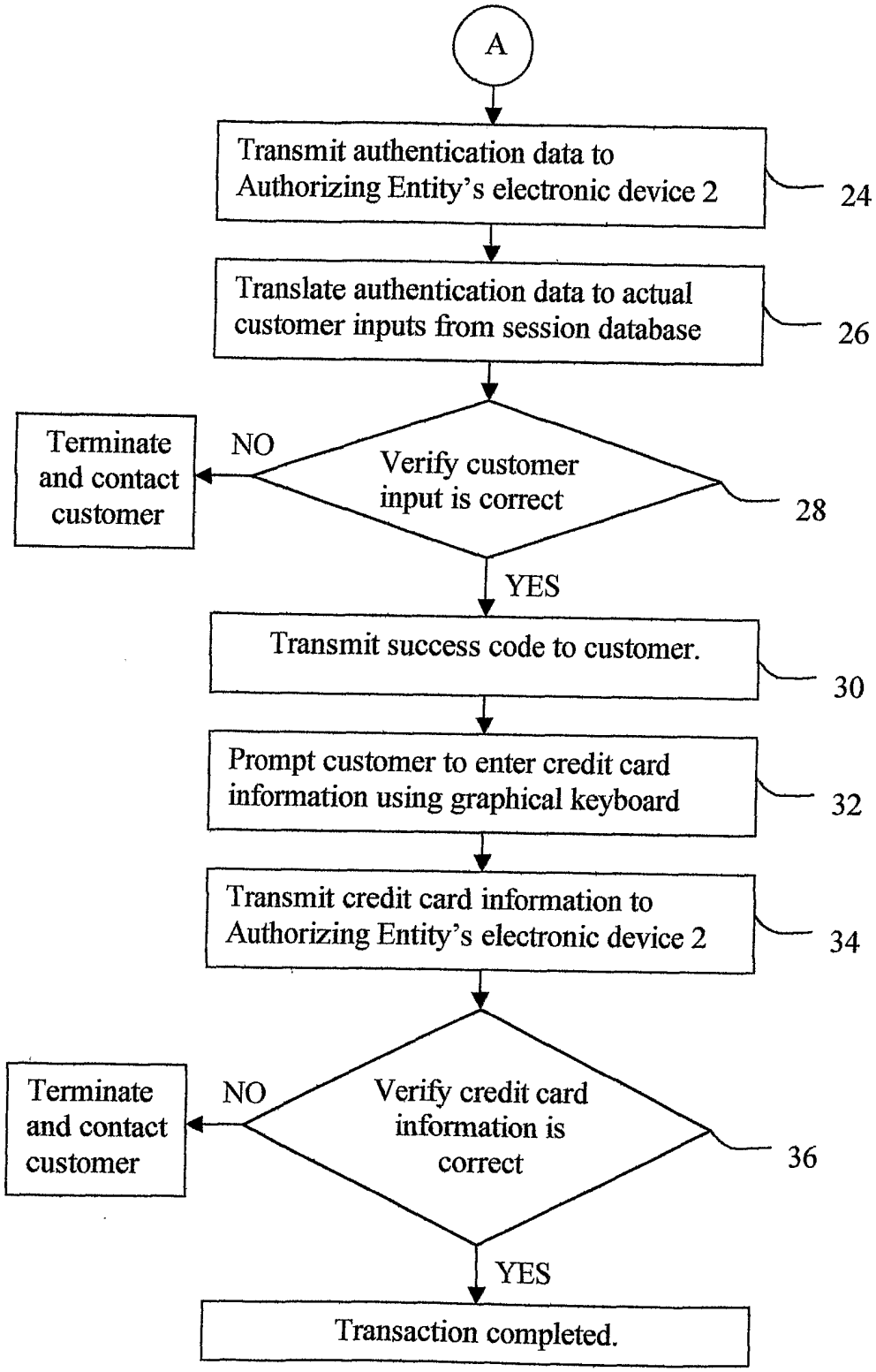
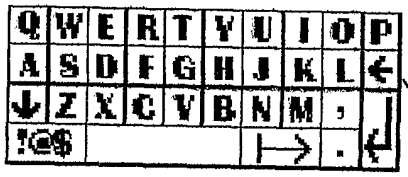
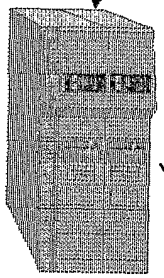

A
Transmit authentication data to Authorizing Entity's electronic device 2
24
Translate authentication data to actual customer inputs from session database
26
Verify customer input is correct
28
NO
Terminate and contact customer
YES
Transmit success code to customer.
30
Prompt customer to enter credit card information using graphical keyboard
32
Transmit credit card information to Authorizing Entity's electronic device 2
34
Verify credit card information is correct
36
NO
Terminate and contact customer
YES
Transaction completed.

Figure 2: Secure Payment for Electronic Transactions

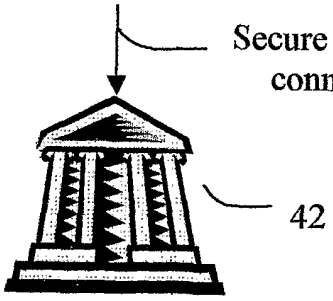


Step 1: Partial credit card information enter through graphical keyboard



Trusted Party

Step 2: Combine pre-stored data with user input



Banks

Figure 3: Protection from unauthorised use

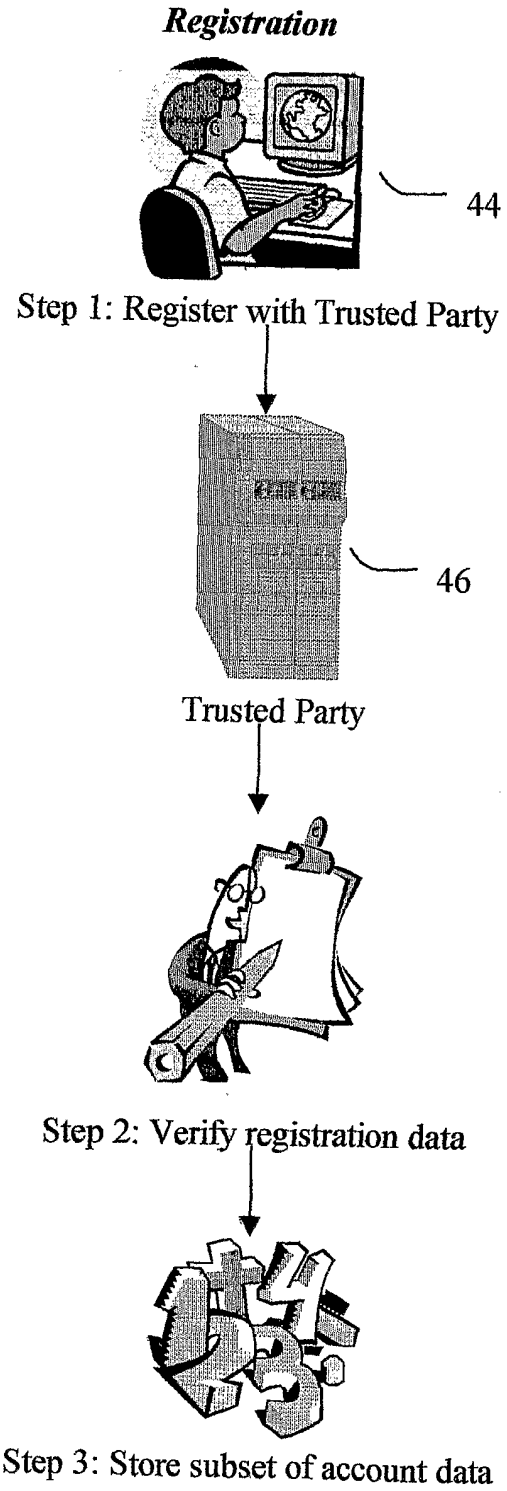
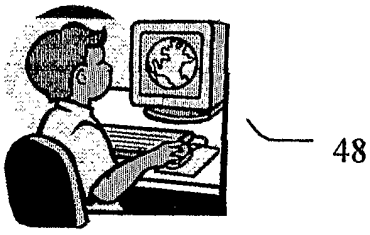
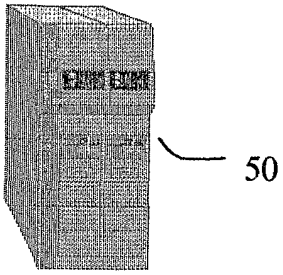


Figure 3: Protection from unauthorised use (Continued)

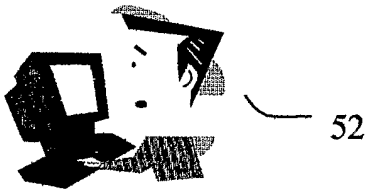
Post-registration



Third / Non-registered party



Step 4: Verify against pre-stored subsets of account data



Step 5: Prompt to login if there is a match