

hardware or software that enables the device to accept a specific response input, usually including buttons which read "approve" and "disapprove." The protocol extension can also optionally include additional security features such as, for example, encryption.

[0012] Another feature is an account profile that is associated with the service of the invention. The user can update the account profile, for example, over a World Wide Web interface. The account profile is checked for each transaction and includes information such as a dollar amount below which the user does not want to be bothered for approvals.

[0013] The invention can be implemented in a network that includes an account processing center which is operable to process transactions in accordance with the payment authorization service that is provided by the invention. In one embodiment, the processing center is connected to a short message service (SMS) system which exchanges messages with the user's device. A merchant network is also connected to the processing center for receiving authorization requests from payees and sending back authorization responses.

[0014] The processing center where credit card processing takes place is typically a large data center with a large computer system or "mainframe" computer. The computer system includes a central processor, a system bus, one or more service processors, and a main memory. There are also input/output (I/O) controllers and large amounts of storage, as well as operator consoles. The specified communication device can take many forms, but typically includes a control block and memory which stores a computer program or "microcode" which operates the device. The control block includes a microprocessor or embedded controller. An input/output block typically includes a keyboard and display. The input/output block can also include keys or buttons for accepting a specialized response input. In the case of a wireless device, an RF unit and antenna allow communication with a wireless network.

[0015] The invention provides exceptional security for credit account transactions because the extra security provided is transparent to payees and merchants. In addition, two seemingly independent and unrelated items must be stolen or cloned in order for a thief to get access to a user's account: the credit account number, and the specified or currently activate approval device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] FIG. 1 is a schematic block diagram of a credit authorization system according to the present invention;

[0017] FIG. 2 is a flowchart showing the method of operation of the authorization system of FIG. 1;

[0018] FIG. 3 is a block diagram of a computer system at the processing center that is used to implement the present invention;

[0019] FIG. 4 is a flowchart showing the method of operation of a wireless device used to respond to an authorization request in accordance with the present invention; and

[0020] FIG. 5 is a schematic block diagram of a wireless device used to implement the present invention.

DETAILED DESCRIPTION

[0021] The present invention provides a system and method for payment authorization. An account user or credit card holder can subscribe to the service to provide more secure credit based transactions. The service uses a communication device specified by the user. The device is typically portable and can include, for example, a two-way pager, cellular telephone with short message service (SMS) capability, a laptop computer or a personal digital assistant. However, the preceding examples are intended to be illustrative, rather than limitations, as any personal communication device, wireline or wireless, can also be used such as, for example, a landline telephone or PC. Through the service, the credit card holder can instruct his or her financial institution not to authorize use of his credit card without electronic authorization via the specified communication device. In doing so, the cardholder specifies to the institution an address for the communication device, e.g. phone number, pager number, IP address, and the like.

[0022] It should be noted that the present invention works with any type of user money account which can be electronically accessed to pay for goods and services. Thus, while credit card accounts are referred to throughout the following discussion, the invention also works with checking accounts, debit accounts, and other types of financial accounts, whether or not a physical "card" is associated with the account.

[0023] Consider, for example, using a credit card to purchase a meal at a restaurant. The user has registered for the service authorization implemented according to the present invention and uses a two-way alphanumeric pager as the specified communication device. The restaurant enters the card number into the system to begin processing for payment, such as, for example, using a card swipe machine. The authorization request containing the appropriate transaction information is sent to the card issuing institution for authorization. As previously discussed, the card processing center portion of the institution runs several tests to verify non-fraudulent card use, to include the approval according to the present invention.

[0024] The processing center determines that the cardholder subscribes to the authorization service and has provided information for a currently specified communications device, in this case a pager. The processing center sends a message to the cardholder's pager and the relevant transaction information appears on the screen. The cardholder, having desired to make the transaction, then uses the two-way capability of the pager to immediately approve the transaction.

[0025] Now, suppose a server at the restaurant writes down the cardholder's credit card number, or captures it on a pocket-sized, card swipe device for later retrieval. Afterwards, the server visits an on-line merchant and enters the stolen card number on a World Wide Web form to pay for the purchase. When an authorization request for this transaction is sent to the processing center for the bank, an approval request is automatically sent to the cardholder as described above. The cardholder, surprised by the approval request, has an opportunity to deny the transaction. Thus, the charge request is intercepted and stopped at the source, preventing the fraud from having significant financial consequences. Meanwhile, the institution has been alerted to the potential fraudulent use of the card and can react quickly.