OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(12) (19) (CA) **Demande-Application**

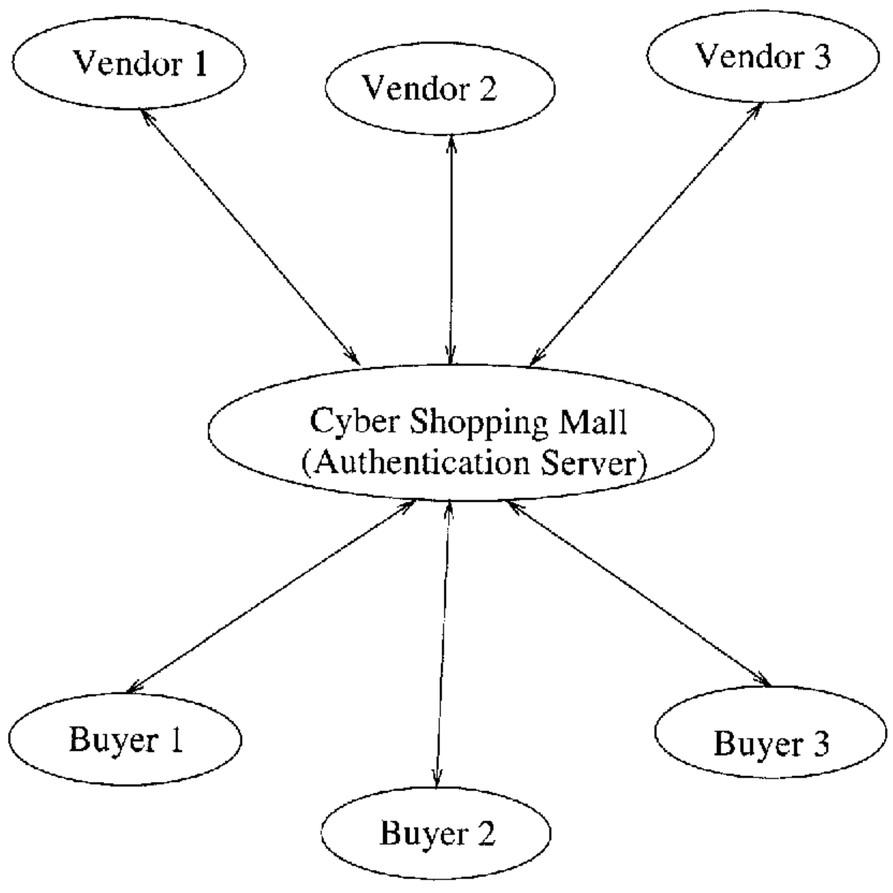
(21) (A1) **2,267,672**
(22) 1999/02/15
(43) 2000/08/15

(72) LU, Tao, CA
(71) LU, Tao, CA

(51) Int.Cl.[6] H04L 9/32, G06F 17/60, G07F 7/12

(54) **METHODE D'AUTHENTIFICATION NUMERIQUE DYNAMIQUE EN FONCTION DES EVENEMENTS ET APPLICATION AUX TRANSACTIONS FINANCIERES CONCLUES SUR L'INTERNET, A L'AUTHENTIFICATION DE L'INSTALLATION DE LOGICIELS, AUX MESURES COURANTES D'AUTHENTIFICATION DES UTILISATEURS DE CARTES BANCAIRES ET DE CARTES DE CREDIT, AINSI QU'AU CONTROLE DE L'ACCES A DISTANCE**

(54) **EVENT DRIVEN DYNAMIC DIGITAL AUTHENTICATION AND ITS APPLICATIONS TO INTERNET FINANCIAL TRANSACTION, SOFTWARE INSTALLATION AUTHENTICATION, ROUTINE CREDIT CARD/BANK CARD USER AUTHENTICATION AND REMOTE ACCESS CONTROL**



Cyber Shopping Protocol

(57) New low risk financial transaction protocols suitable to both Internet and routine financial trading are defined. An authentication method using event drive dynamic digital authentication card is used. The payment method on Internet is disclosed. The seller owns an on-line shopping store on a Cyber Shopping Mall.The customer can visit the seller's store via shopping mall's frame. On paying for the transaction, the Cyber Shopping Mall's authentication server will ask the customer for confirmation. The buyer replies with the appropriate PIN for authentication. The PIN is a combination of event counter and a pseudo random number sequence generated by an authentication card. On each

OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(21) (A1) **2,267,672**
(22) 1999/02/15
(43) 2000/08/15

transaction, the customer trigger the card to obtain an distinct random number and the event counter is increased by one. He then key-in the event counter and the random number sequence as the PIN. By checking the PIN in the authentication server's database, the server can tell if the customer is the true card holder. It can then finish the transaction between the customer and the vendor's account stored in the server's database. Such an authentication method can also be used in the software installation authentication to prevent unauthorized installation of software. To facilitate the key-in of the PIN, an optical card reader is described in this invention. The use of dynamic PIN authentication, furthermore, can be also used in routine financial transaction like direct payment using a bank card or credit card payment on daily shopping to prevent card fraud. The transaction and authentication protocols described in this invention is highly reliable and simple, which makes it a promising solution on secure e-commerce.

Event Driven Dynamic Digital Authentication and Its Applications to Internet Financial Transaction, Software Installation Authentication, Routine Credit Card/Bank Card User Authentication and Remote Access Control

Tao Lu

Tel: 613 282-4833

E-mail: lut_1998@yahoo.com

February 13, 1999

Address: 98 Bagot St. Apt. 5
Kingston. ON K7L 3E5

Abstract

New low risk financial transaction protocols suitable to both Internet and routine financial trading are defined. An authentication method using event drive dynamic digital authentication card is used. The payment method on Internet is disclosed. The seller owns an on-line shopping store on a Cyber Shopping Mall.The customer can visit the seller's store via shopping mall's frame. On paying for the transaction, the Cyber Shopping Mall's authentication

server will ask the customer for confirmation. The buyer replies with the appropriate PIN for authentication. The PIN is a combination of event counter and a pseudo random number sequence generated by an authentication card. On each transaction, the customer trigger the card to obtain an distinct random number and the event counter is increased by one. He then key-in the event counter and the random number sequence as the PIN. By checking the PIN in the authentication server's database, the server can tell if the customer is the true card holder. It can then finish the transaction between the customer and the vendor's account stored in the server's database. Such an authentication method can also be used in the software installation authentication to prevent unauthorized installation of software. To facilitate the key-in of the PIN, an optical card reader is described in this invention. The use of dynamic PIN authentication, furthermore, can be also used in routine financial transaction like direct payment using a bank card or credit card payment on daily shopping to prevent card fraud. The transaction and authentication protocols described in this invention is highly reliable and simple, which makes it a promising solution on secure e-commerce.

Background of the Invention

As the Internet is exploding at the beginning of the next millennium, e-Commerce is blooming. In 1997, an estimated $ 1.8 billion worldwide online shopping revenues is reported. Retail revenues of online shopping worldwide are forecasted increase to $200 billion by 2001. However, with the grow-up of the market, simple, secure online payment method still remains a question. Currently, numerous e-payment methods have been proposed, these include CyberWallet, eCash, netCash and PayMe Transfer Protocol, etc. Although most methods provide full security protection, they all have some drawbacks as either too complicated for merchants or customers to install such software or not scalable. This invention will define a new online payment method. Using this method, no credit card information will be

transferred through the Internet and no complicated software needs to be installed on either customers' or merchants' side. With the use of dynamic digital authentication card, the customer can virtually go shopping, check the financial statement or write a cybercheque from anywhere via a web browser. Furthermore, this transaction system is not only limited on Internet transaction, it can be used to replace the conventional credit card or direct payment method during our daily routine trade to avoid credit card or bank card fraud. By using the card reader of the invention, the customer can facilitate the key-in of an authentication card PIN number to the computer. One more application of dynamic digital authentication is in the field of software installation authentication to prevent the software privacy.

Brief Summary of the Invention

This invention comprises of one defined dynamic digital authentication system and its application to several Internet financial transaction protocols and one software installation protocol. The dynamic digital authentication system is defined as a security card with PIN changing on each event or also known as dynamic PIN hold by a user and a server to certify the PIN entered by the user is correct. The dynamic PIN verification system provides a strong authentication method over open network such as Internet. Using this authentication system, several Internet financial transaction protocols are defined as IFT, which the server is mainly performed as both authentication and financial institute. In the Cyber Shopping Mall (CSM), the authentication server sits between the customer and vendor, and performs more like a virtue shopping mall. Besides, this invention describes an Internet Fund Transfer and Cyber Check protocol to provide authentication on Internet fund transfer. This invention further describes an authentication method in replacement of routine credit card transaction authentication method. The last part of the invention is the software installation authentication applied to against unauthorized software piracy. This system can also used

in remote access control.

Brief Description of Drawings

Figure 1 illustrates the Format of PIN;

Figure 2 illustrates Dynamic Digital authentication Card Reader;

Figure 3 illustrates an Internet Financial Transaction Protocol;

Figure 4 illustrates Cyber Shopping Protocol, and

Figure 5 illustrates Software Installation Authentication

Detailed Description

Event Driven Dynamic Digital Authentication System

The hardware required by this invention is an event driven dynamic digital authentication system, namely, a dynamic authentication card hold by each user, an optional card reader to facilitate the input of PIN and a sever to perform the authentication. The card is virtually a pseudo random number sequence generator. It can also be installed in watches, electronic address books, palm pilots or home PC in either hardware or software form. The PIN displayed on the card is as described in Figure 1, it is formed by two parts, a 2 digit event id and a 6 digit random number. On each time of transaction, the event id increased by one according to $EventCounter_{n+1} = (EventCounter_n + 1) mod 100$. The seed of the random number generator for each individual card is kept privately by the authentication sever so it is the only part that can reproduce the PIN other than the card itself. During the process of authentication, the server queries the account name and the PIN of the user via an open network such as Internet, the server then compute the PIN to see if it matches the number input by the user. If the match is positive, then the server determines the account user is the

proper card holder and authentication is completed. Since the PIN is generated by the card and only reproducible by the server, the information transmitted through the open network is secured. That is, even the third party intercepts the PIN on the network, he/she can not reproduce it in the future and thus, becomes useless information to the third party. If the card is lost or stolen, then person who gets the card can't use it without the knowledge of the account name of the card-holder. Meanwhile, the card itself can be password protected, that is, it only displays the PIN when you key in the password. This effectively prevents the malicious steal by someone who is familiar with the card-holder and knows his account name.

As the PIN is formed by 8 digits, an optional card reader described below is preferable to speed up the input of the PIN. The authentication card reader in this invention facilitates reading in the PIN generated by the card. As key in a string of digits is tedious, the reader provides a faster means to read the PIN. The scheme of the reader is shown in Fig. 2; the authentication card has a sensor switch and an L.E.D. The photo diode or a micro mechanical sensor. The figure shows the sensor as a photo diode. If the card is not in the reader, the switch is off. When we insert the card to the reader, the sensor will detect light from the reader indicator. It then triggers the gate "on" so that the serial PIN signal can pass the gate and modulate the L.E.D to emit light pulses. As the insertion of the card also triggers the sensor of the reader to turn on the photo diode 2 in "read" state, photo diode 2 then detects the light pulse train and decodes it into digital signal and sends to the computer.

Overall, the authentication process described above has significant improvement over conventional password authentication method.

This invention describes several protocols for Internet financial transaction, software installation authentication, remote access control and routine credit card transaction. All the

protocols require the dynamic digital authentication systems described above. The initial stage is to setup the authentication and transaction system. A server should reside in a site maintained by a financial institution known as Credit Processor, and such site should be accessible by any user via Internet. To apply the membership of the authentication system, the user sends out personal information including credit card number, date of birth, etc. to the credit processor. This should be done off-line of by sending encrypted message to keep the privacy of such information. Upon reviewing the application, the credit processor then grants the user a specific account name and a dynamic digital authentication card. The user's information will be saved in the secure database maintained by the credit processor. The card will serve the user as both the personal ID and credit card in the protocols listed as following.

A. Internet Financial Transaction (IFT) Protocol

The first protocol is the Internet financial transaction protocol used in on-line shopping, also known as e-commerce. Fig. 3 shows the overall electronic Internet Financial Transaction (IFT) protocol. The Online payment system is described as below:

1. The customer (the buyer) visits a registered cyber store and buys some items. At the stage to pay for the order, the seller posts the total price on the buyer's browser and asks for confirmation and the buyer's account name. The buyer should also have chances to justify or reject the purchase at this point. If the buyer is satisfied with the price, he then replies the confirmation message with his account name attached.

2. Upon receiving the confirmation message, the seller then composes and sends a formatted message to the credit processor to validate the transaction. The message should include both buyer's and seller's account name, the amount of the transaction and the IP address the buyer is logging on.

3. The credit processor after receiving the message posts the transaction to the buyer's browser directly and asks for confirmation and authentication. The buyer then trigger the authentication card to generate a new PIN and sends the confirmation back to the credit processor with the authentication PIN attached. If the credit processor does not receive the confirmation within a time window or the authentication PIN does not match the PIN generated by the credit processor server after several trials, this transaction will be discarded and the invalidated confirmation will be sent to the seller. The transaction should also be discarded if the buyer's account is over-limited.

4. On the other hand, if the confirmation is received with the proper PIN, the credit processor will confirm the transaction with the seller. After knowing that the seller has received the confirmation, the credit processor then update the database to complete the transaction with the two accounts.

5. After receiving the confirmation from the credit processor, the seller can then finalize the transaction by sending out the items ordered to the buyer.

6. The messages communicating between the parties are encrypted by standard means (SSL) to have a first level protection. Since the account information is stored in private database of the credit processor, no sensitive information will propagate over the Internet. It virtually eliminates the possibility that information like date of birth, credit card number etc., be intercepted by the unanticipated party or even by the seller. The risk of credit card or bank-card fraud will even be much lower than conventional credit card payment method in our daily life. Also, we assume prohibiting the reuse of one PIN, that is, after one purchase, the buyer shouldn't make another purchase before updating the PIN. Even the third party intercepts the account name and PIN, it becomes impossible for him to use this information to perform a fraudulent use since his false transaction is always check in late than the true one. In the worst case that

the unanticipated party does succeed in a fraud, it is easy to trace him out since all the transaction are done within the registered accounts.

B. Cyber Shopping Mall (CSM) Protocol

An alternative protocol called Cyber Shopping Mall (CSM) Protocol is shown in Fig. 4. The authentication server now resides in a cyber shopping mall site. The customer can land on the site and visit vendor's store via shopping mall's frame. The payment transaction is directly performed between the server and the buyer, and thus simplify the steps described by the IFT protocol.

C. Internet Fund Transfer and Cyber Check

Although the above description is for Internet shopping, this payment system is also suitable for other e-commerce transactions; namely, a customer can transfer fund to another registered customer's account on the Internet using authentication card. Also it's possible to generate a cyber check to an unregistered customer. For example, a person A can issue or register a check payable to person B at the credit processor authenticated by his PIN. Then he can print a copy of the check out and hand it to B. Person B can then deposit it to his bank account as a real check. The check can then be cleared between the bank and the credit processor.

D. Replacement of Routine Credit Card

Use of the dynamic authentication system is also a good replacement of conventional credit card and direct payment method. Conventionally, the credit card number or bank card number is statically read into merchant's card reader, and the bank card holder may then key in his/her password to authenticate. However, the merchant may intercept the card number

and/or password. This is the main source of credit card fraud. By using the authentication card, the PIN now becomes dynamic, that means, even the merchant intercept the PIN, he/she can not reuse it unless he/she can decipher the cryptology. This will significantly lower the risk as using the conventional means of credit card transaction. In the case the digital authentication card is lost by the customer, the person who finds it unless he knows the card owner's account name can not use it.

E. Software Installation Authentication Protocol

Another application of the dynamic authentication system is in software installation authentication. As the current protection against software piracy is poor, anyone with a hard copy of CD key can easily install pirated software with little difficulty. In this new protocol, a customer is assumed to own an authentication card and each software CD is distinguished by a serial code. The software in the CD is encrypted by conventional cryptography method. The key can be stored in the CD or obtained from the manufacturer. At the first installation of the software, the installation program will query the customer's account name and the dynamic PIN displayed on the card. The setup program then sends the information to manufacturer's server via a modem. The manufacturer's server then forwards the information to authentication server for validation. After received the positive confirmation, the manufacturer's server will then grant the access of private key for the CD to the setup program and register the CD according to its serial number. The setup program can then decrypted the CD and install the software. In the case the authentication result is negative or some other users previously register the CD, the CD will be considered as pirated and the setup program will stop installing the software.

F. Remote Access Control

The event driven dynamic digital PIN authentication can also be used in remote access control. Similar product is available from Security Dynamics' remote access control card. Such card update the PIN every 6 seconds, which is inconvenient for the user to keyin the PIN. Using event driven PIN, the user trigger a new PIN only when he attemps to login his account. It's much more convenient than the formerly described method since the PIN won't change in a short time window.

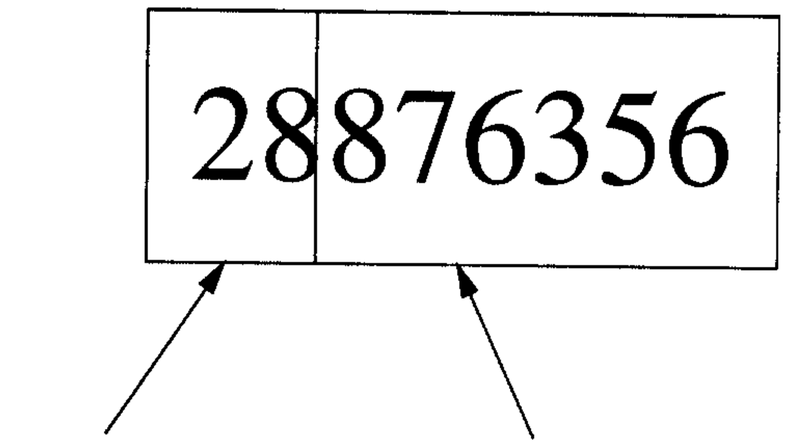
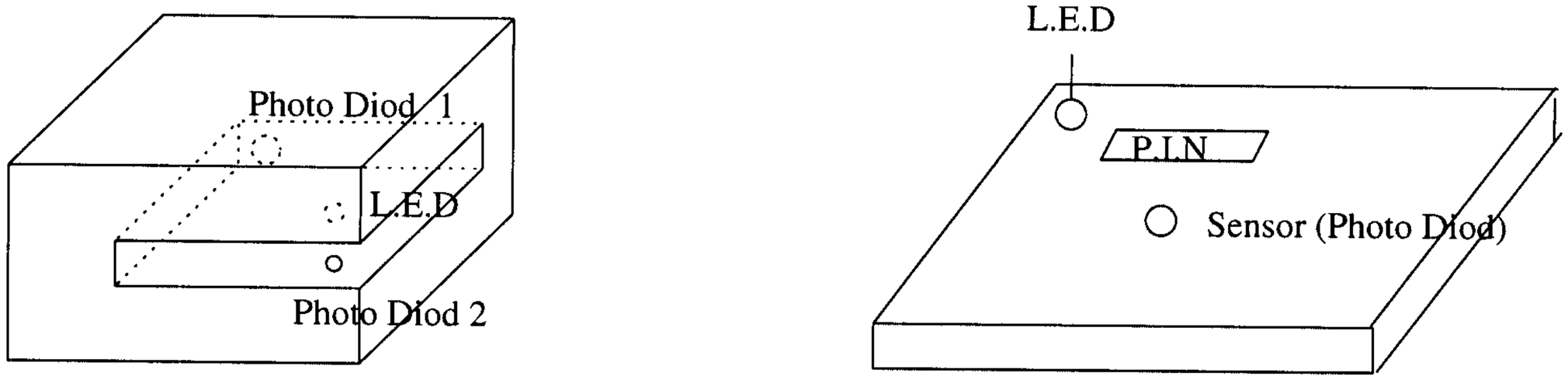


Figure 1: Format of the PIN



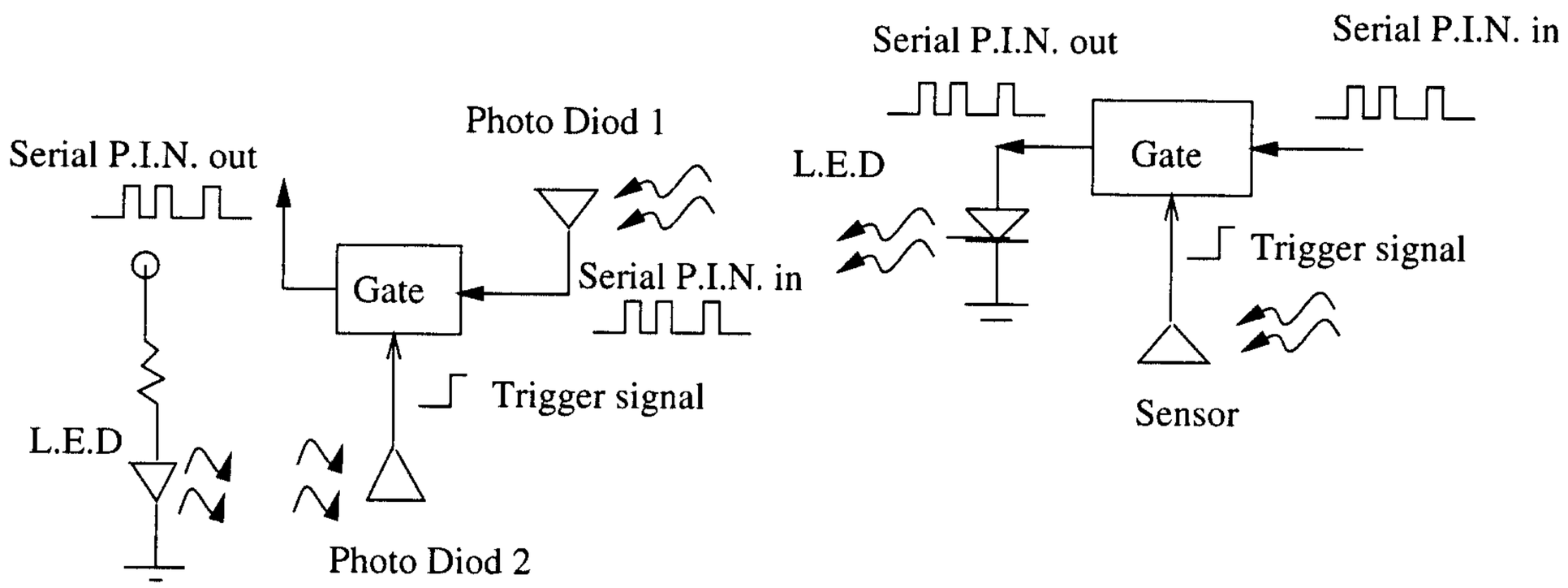


Figure 2: Dynamic Digital Authentication Card Reader

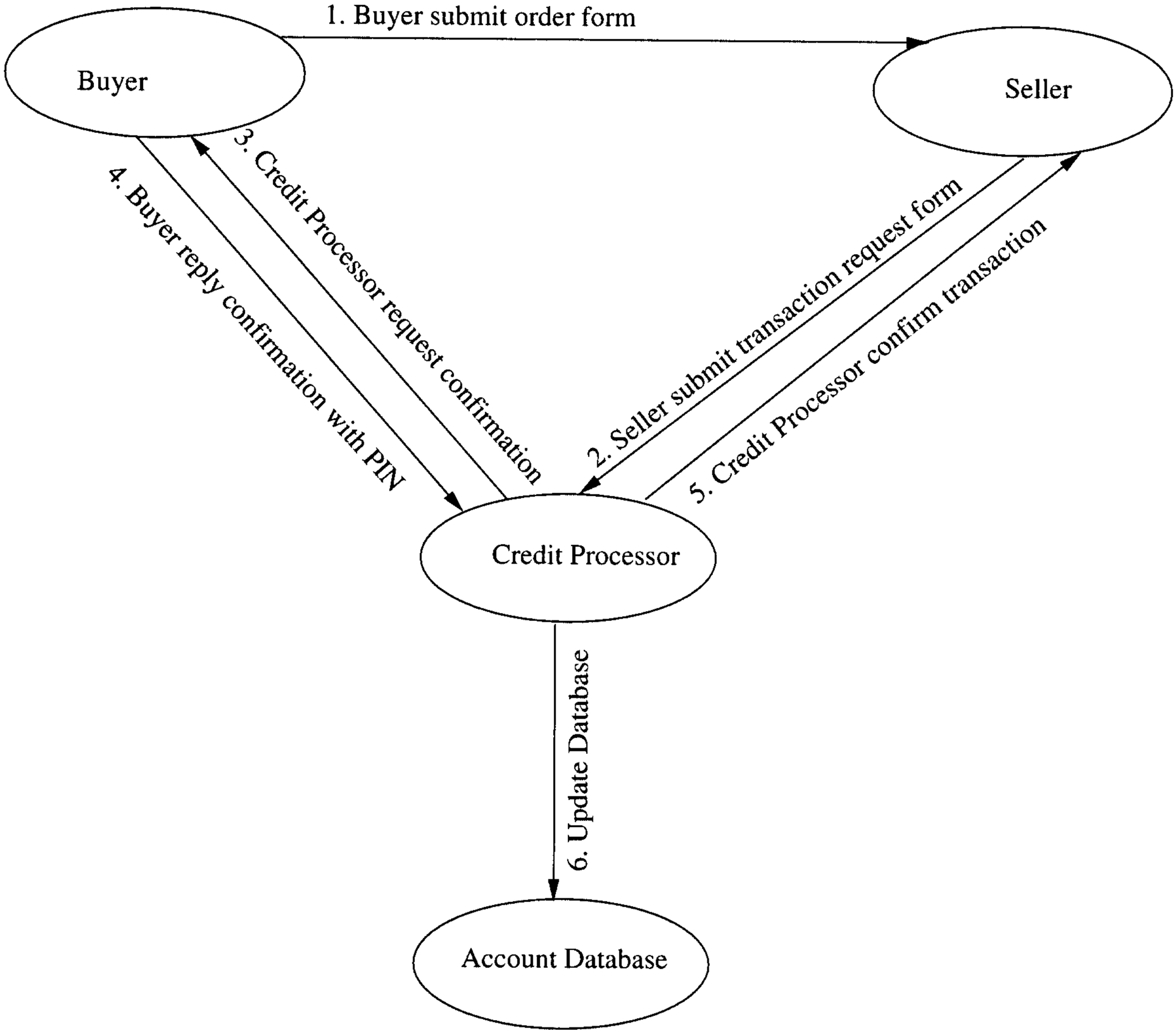


Figure 3: An Internet Financial Transaction Protocol

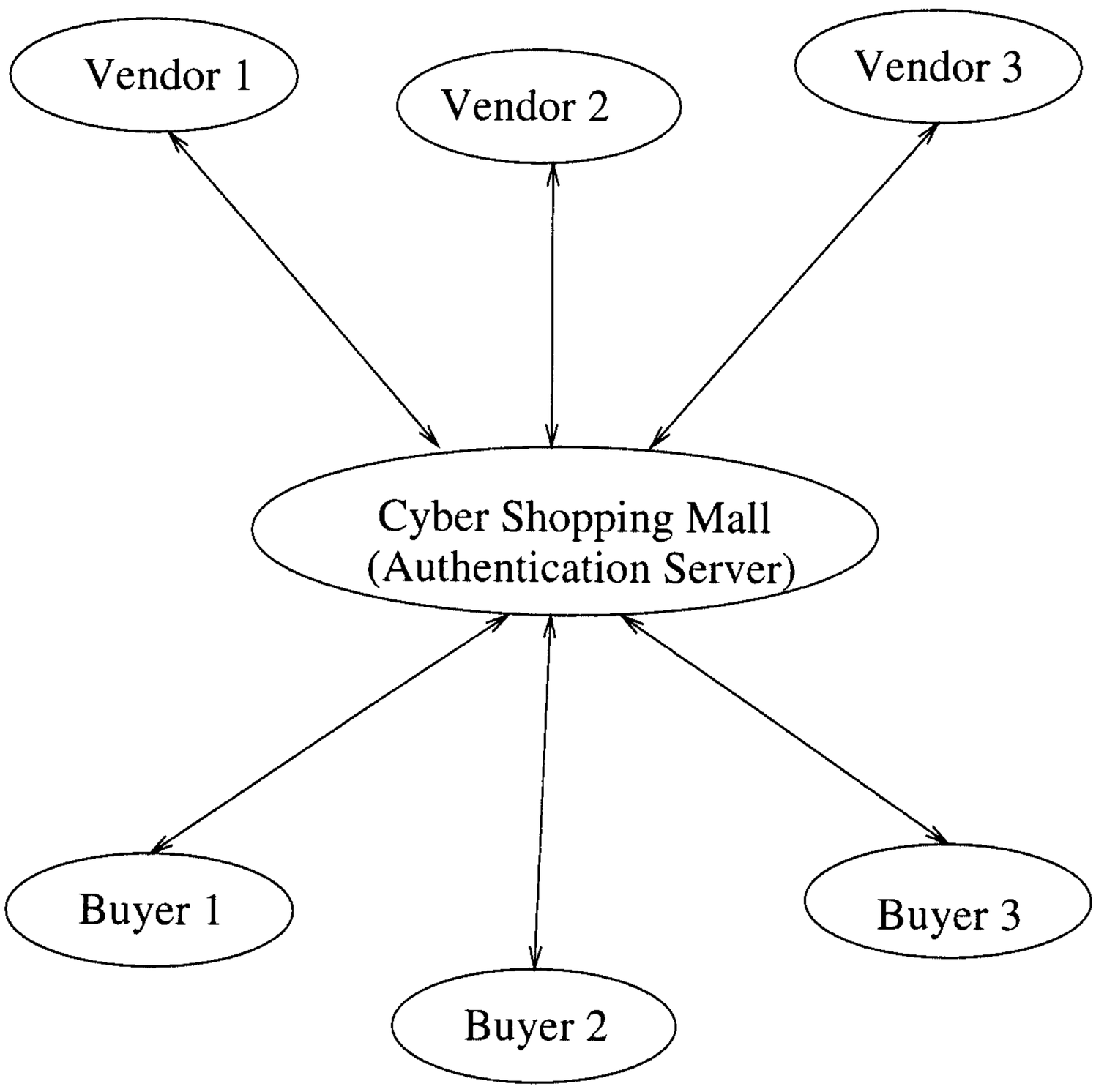


Figure 4: Cyber Shopping Protocol

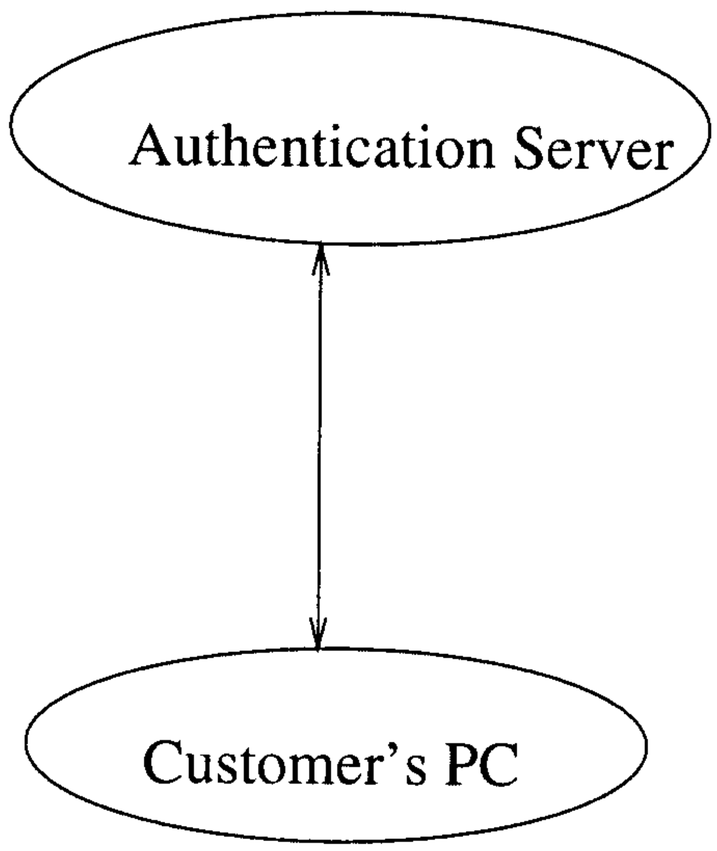


Figure 5: Software Installation Authentication