Title

Updating a mobile payment device

Technical Field

The invention concerns a system for updating a mobile payment device of a user via an insecure network.

Background of the Invention

Ticketing for mass transit systems must be efficient to ensure good traffic flow of commuters as they enter and exit the transit system. One type of ticket is a reusable stored value card which is carried by the commuter for ticketing of all trips. To alleviate bottlenecks at entry and exit gates, the card is contactless which enables it to be quickly scanned as the commuter passes through the gates and debited when the commuter has completed their journey.

Although this bottleneck is addressed, another is created at top-up stations for replenishing the value of the card. Typically, at a top-up station, the commuter inserts their card and makes payment via cash or credit/debit card to add value to their card. Top-up stations are bulky since they must be able to securely store and dispense large amounts of cash. In subway stations, there is an acute lack of space and thus there are a limited number of top-up stations present. Thus long queues during peak hour periods may form which not only delays the commuter but occasionally obstructs traffic within the station. A simple solution has been to place top-up machines outside the station. Commuters find this inconvenient so they are not frequently used.

Thus there exists a need to further increase the efficiency of mass transit systems.

Furthermore, a large proportion of the public have these cards, and thus in certain countries they may also be used for cashless payment for products and services at participating outlets. However, the popularity for these alternative uses is limited as the problem remains in finding a top-up station to replenish their card, conveniently.

Summary of the Invention

166166

G00002

In a first preferred aspect, there is provided a method for updating a mobile payment device of a user via an insecure network, the mobile payment device storing value and enabling the user to perform cashless transactions with participating merchants, the method comprising:

transmitting identification information relating to the mobile payment device to an authentication server;

authenticating the mobile payment device with the authentication server; and

selecting a transaction type and transaction amount for a transaction;

wherein authentication comprises:

transmitting an encrypted first message from the authentication server to the mobile payment device, and an encrypted second message from the mobile payment device to the authentication server;

decrypting the encrypted first and second messages;

transmitting an encrypted third message based on the first message from the mobile payment device to the authentication server, and an encrypted fourth message based on the second message from the authentication server to the mobile payment device;

decrypting the encrypted third and fourth messages; and

comparing the first message with the third message and the second message with the fourth message, where if they match, the identity of the mobile payment device and the authentication server are authenticated with each other to enable updating of the mobile payment device in accordance with the transaction.

The method may further comprise the initial step of placing the mobile payment device on or near a reader device to read the identification information relating to the mobile payment.

The method may further comprise establishing a communication link between the mobile payment device and the authentication server via a client application.

The client application may be downloaded to a client terminal of the user.

The client application may be an applet for execution within an Internet browser application.

The mobile payment device may be a contactless integrated chip card.
The mobile payment device may be a contactless smart card (CSC).

The participating merchants may include public transport authorities and retail outlets.

The transaction type may be any one in the group consisting of: refund, adding value to the mobile payment device, and updating electronic data stored on the mobile payment device.

Communication between the authentication server and the mobile payment device may be via Application Protocol Data Unit (APDU) packets.

The method may further comprise establishing communication between the authentication server and a bank host to debit or credit a bank account of the user in accordance with the transaction.

The insecure network may be the Internet, Metropolitan Area Network (MAN), or Wide Area Network (WAN).

In a second aspect, there is provided a system for updating a mobile payment device of a user via an insecure network, the mobile payment device storing value and enabling the user to perform cashless transactions with participating merchants, the system comprising:

an authentication server to authenticate the mobile payment device;

a reader device to read identification information from the mobile payment device;

a client terminal to transmit the identification information to the authentication server via the network; and

a user interface to enable selection of transaction type and transaction amount for a transaction;

wherein authentication comprises:

transmitting an encrypted first message from the authentication server to the mobile payment device, and an encrypted second message from the mobile payment device to the authentication server;

decrypting the encrypted first and second messages;

transmitting an encrypted third message based on the first message from the mobile payment device to the authentication server, and an encrypted fourth message based on the second message from the authentication server to the mobile payment device;

decrypting the encrypted third and fourth messages;

comparing the first message with the third message and the second message with the fourth message, where if they match, the identity of the mobile payment device and the authentication server are authenticated with each other to enable the reader device to update the mobile payment device in accordance with the transaction.

The mobile payment device may be a contactless integrated chip card.
The mobile payment device may be a contactless smart card (CSC).

The reader device may be a Universal Serial Bus (USB) type contactless card reader/writer.

In a third aspect, there is provided an applet for enabling a mobile payment device of a user to be updated via an insecure network, the mobile payment device storing value and enabling the user to perform cashless transactions with participating merchants, the applet comprising:

a user interface to allow the user to select a transaction type and transaction amount for a transaction;

a server communications module to communicate with an authentication server for authenticating the mobile payment device; and

a device communications module to interface with a reader device to read and update the mobile payment device;

the server communications module facilitating authentication by: receiving an encrypted first message from the authentication server to be decrypted by the mobile payment device, and receiving an encrypted fourth message based on the second message from the authentication server to be decrypted by the mobile payment device;

the device communications module facilitating authentication by: transmitting an encrypted second message from the mobile payment device to the authentication server to be decrypted by the authentication server; transmitting an encrypted third message based on the first message from the mobile payment device to the authentication server, to be decrypted by the authentication server;

wherein the first message is compared with the third message and the second message is compared with the fourth message, where if they match, the identity of the mobile payment device and the authentication server are authenticated with each other to enable the reader device to update the mobile payment device in accordance with the transaction.

The applet may be a signed Java applet downloadable to a client terminal of the user.

Advantageously, the present invention provides users with flexibility and the ability to leverage their computer to perform e-services using their mobile payment device for cashless transactions in a secure manner.

Brief Description of the Drawings

An example of the invention will now be described with reference to the accompanying drawings, in which:
Figure 1 is a system architecture diagram of the system in accordance with the present invention;
Figure 2 is a use case diagram of downloading an applet to the client terminal of the user to interface between the authentication server and the card of the user;
Figure 3 is a use case diagram of establishing communication between the authentication server and the card;
Figure 4 is a use case diagram of performing an update to the card; and
Figure 5 is a process flow diagram of the authentication process in accordance with the present invention.

Detailed Description of the Drawings

Figure 1 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the present invention may be implemented. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a personal computer. Generally, program modules include routines, programs, characters, components, data structures, that perform particular tasks or implement particular abstract data types. As those skilled in the art will appreciate, the invention may be practiced with other computer system

configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable user electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

Referring to Figures 1 to 4, a system 10 for updating a contactless smart card (CSC) 5 of a user over the Internet is provided. The CSC 5 stores value, that is, it contains a cash value for payment of purchases. The CSC 5 enables the user to perform cashless transactions with participating merchants within a cashless network. The participating merchants include public transport authorities 50 and retail outlets such as zoos 60, movie cinemas 70 and hospitals 80, which may be accessed via their web servers. In a typical scenario, the user presents their CSC 5 to a participating merchant for payment, it is read, and an appropriate amount is deducted from the stored value of the CSC 5.

The system 10 comprises: an authentication server 20, a USB type contactless card reader/writer 30 connected to a desktop or notebook computer 40 of the user. It is assumed that the appropriate drivers for the card reader/writer 30 have been installed on the computer 40. The authentication server 20 authenticates the CSC 5. The authentication server 20 is operated by an e-services provider which also manages the distribution of the CSCs 5 in the market and ensures participating merchants are adequately supported within the cashless network. E-services include viewing the CSC 5 details, viewing transaction history of the CSC 5, top-up of CSC 5, refund of CSC 5, personalising the CSC 5, loyalty schemes, payment of e-ticketing/coupons, viewing medical history, access logon and booking appointments. Technical support is provided to the participating merchants in the form of hardware to correctly read/write to the CSCs 5 of users.

The card reader/writer 30 may be an ACR120 Contactless Reader manufactured by Advanced Card Systems Ltd based in Hong Kong. The card reader/writer 30 reads identification information from the CSC 5, and writes to the CSC 5 to update it. Wireless communication between the CSC 5 and the card reader/writer 30 is via ISO 14443-C Felica.

The computer 40 communicates with the authentication server 20 via the Internet. Prior to allowing transactions and updates to the CSC 5 to occur, both the authentication server 20 and CSC 5 must authenticate and verify the identity of themselves to each other.

Referring to Figure 5, the authentication process 200 involves the authentication server 20 and CSC 5 each generating 201 a random number. A copy of the random number is stored temporarily for comparison later. The random numbers in plain text are encrypted 202 by a predetermined encryption algorithm. The encryption algorithm may be a private key (symmetric) encryption such as the Advanced Encryption Standard (AES) using a secret key of 128, 192, or 256 bits. The authentication server 20 transmits 203 its encrypted random number in a message to the CSC 5 via the computer 40. The CSC 5 transmits 203 its encrypted random number in a message to the authentication server 20. When the messages are received by the CSC 5 and the authentication server 20, they are opened and the random number contained in the message is decrypted 204 by the decryption function of the predetermined encryption algorithm. Again, the random numbers are encrypted 205 by the predetermined encryption algorithm and transmitted 206 in a message to the CSC 5 and authentication server 20, respectively. When the messages are received by both the CSC 5 and the authentication server 20, they are opened and the random number contained in the message is decrypted 207 by the decryption function of the predetermined encryption algorithm. The random number received and decrypted by the CSC 5 is compared 208 with the temporary copy generated by the CSC 5 earlier. If there is a match, the identity of the authentication server 20 has been verified to the CSC 5. At this point, the authentication process is only partially successful. Similarly, the random number received and decrypted by the authentication server 20 is compared with the temporary copy generated by the authentication server 20 earlier. If there is a match, the identity of the CSC 5 has been verified to the authentication server 20. When both identities have been verified, authentication is successfully completed 209 and the card reader/writer 30 is permitted 210 to update the CSC 5.

As CSCs 5 generally have limited storage capacity, the encryption algorithms are preferably small in size and not complex. To satisfy user friendliness, the authentication process is fast and effective, and is transparent to the user.

However, the authentication process is robust to withstand possible security breaches.

In a typical scenario, with reference to Figure 2, the user launches an Internet browser application and inputs the URL address to access the authentication server 20. Alternatively, rather than directly accessing the authentication server 20 initially, the user may connect to the authentication server 20 via a dedicated web server 100. In response to the HTTP request, the web server 100 serves a web page to the user providing them with instructions to download an applet for e-services using their CSC 5. The applet is digitally signed by a trusted party to ensure authenticity. Once the applet has completed downloaded to the user's computer 40, a security dialog box appears to request confirmation from the user to execute the applet. When the applet is executed, it enters a power up mode, detects and establishes a connection with the card reader/writer 30.

Turning to Figure 3, after the applet is downloaded and executing in a window o the Internet browser, the user places the CSC 5 on or near the card reader/writer 30 for reading. The identification information of the CSC 5 is retrieved by the card reader/writer 30 and transmitted by the computer 40 to the authentication server 20. Based on the CSC 5, the authentication process described earlier is performed. In one embodiment, the authentication process is performed using Application Protocol Data Unit (APDU) packets.

Turning to Figure 4, after successful authentication, all necessary connections are now established and the applet switches from the power up mode to a service mode. The CSC 5 is ready for reading and writing. The applet displays a screen which allows the selection of transaction type and transaction amount for a transaction using the CSC 5. For example, the user wants to add value to their CSC 5. The user selects "add value" as the transaction type and enters "$10" as the transaction amount. The user also selects payment mode, in this example, a credit card, and then inputs the credit card number and expiry date. A message is constructed containing the transaction type, transaction amount, payment mode and payment details of the user. The message is transmitted to the authentication server 20. On receiving the message, the authentication server 20 deconstructs the message and forwards the payment details and transaction amount to the issuing bank 90 of the user's credit card. When the issuing bank returns an approval for the debit request, the authentication server 20 generates "write" APDU

packets and transmits via the computer 40 to update the CSC 5. Once the CSC 5 has been updated with the added value, the transaction is completed. The user may then proceed to use their CSC 5 with the additional $10 in stored value at participating merchants.

In a similar manner, other transaction types are available, including refund to the user's bank account, online payments for e-commerce and recent transaction activity of the CSC 5.

Although a CSC 5 has been described, it is envisaged other mobile payment devices are possible including contact and contactless integrated chip cards.

Although an applet has been described, a dynamic web page may also be the user interface. To ensure security, secure sockets layer (SSL) may be used to encrypt the web page in transit over the Internet.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the scope or spirit of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects illustrative and not restrictive.

WE CLAIM:

1. A method for updating a mobile payment device of a user via an insecure computer network, the mobile payment device storing value and enabling the user to perform cashless transactions with participating merchants, the method comprising:

transmitting identification information relating to the mobile payment device to an authentication server;

authenticating the mobile payment device with the authentication server; and

selecting a transaction type and transaction amount for a transaction;

wherein authentication comprises:

transmitting an encrypted first message from the authentication server to the mobile payment device, and an encrypted second message from the mobile payment device to the authentication server;

decrypting the encrypted first and second messages;

transmitting an encrypted third message based on the first message from the mobile payment device to the authentication server, and an encrypted fourth message based on the second message from the authentication server to the mobile payment device;

decrypting the encrypted third and fourth messages;

comparing the first message with the third message and the second message with the fourth message, where if they match, the identity of the mobile payment device and the authentication server are authenticated with each other to enable updating of the mobile payment device in accordance with the transaction; and

establishing a communication link between the mobile payment device and the authentication server via a client application, the client application being downloaded to a client terminal of the user upon authentication.

2. The method according to claim 1, further comprising the initial step of placing the mobile payment device on or near a reader device to read the identification information relating to the mobile payment.

3. The method according to claim 1, wherein the client application is an applet for execution within an Internet browser application.

4. The method according to claim 1, wherein the mobile payment device is a contactless integrated chip card.

5. The method according to claim 4, wherein the mobile payment device is a contactless smart card (CSC).

6. The method according to claim 1, wherein the participating merchants include public transport authorities and retail outlets.

7. The method according to claim 1, wherein the transaction type is any one in the group consisting of: refund, adding value to the mobile payment device, and updating electronic data stored on the mobile payment device.

8. The method according to claim 1, wherein communication between the authentication server and the mobile payment device is via Application Protocol Data Unit (APDU) packets.

9. The method according to claim 1, further comprising establishing communication between the authentication server and a bank host to debit or credit a bank account of the user in accordance with the transaction.

10. The method according to claim 1, wherein the insecure network is the Internet, Metropolitan Area Network (MAN), or Wide Area Network (WAN).

11. A system for updating a mobile payment device of a user via an insecure computer network, the mobile payment device storing value and enabling the user to perform cashless transactions with participating merchants, the system comprising:

an authentication server to authenticate the mobile payment device;

a reader device to read identification information from the mobile payment device;

a client terminal to transmit the identification information to the authentication server via the network; and

a user interface to enable selection of transaction type and transaction amount for a transaction;

wherein authentication comprises:

transmitting an encrypted first message from the authentication server to the mobile payment device, and an encrypted second message from the mobile payment device to the authentication server;

decrypting the encrypted first and second messages;

transmitting an encrypted third message based on the first message from the mobile payment device to the authentication server, and an encrypted fourth message based on the second message from the authentication server to the mobile payment device;

decrypting the encrypted third and fourth messages;

comparing the first message with the third message and the second message with the fourth message, where if they match, the identity of the mobile payment device and the authentication server are authenticated with each other to enable the reader device to update the mobile payment device in accordance with the transaction; and

establishing a communication link between the mobile payment device and the authentication server via a client application, the client application being downloaded to the client terminal of the user upon authentication,

12. The system according to claim 11, wherein the mobile payment device is a contactless integrated chip card.

13. The system according to claim 12, wherein the mobile payment device is a contactless smart card (CSC).

14. The system according to claim 13, wherein the reader device is a Universal Serial Bus (USB) type contactless card reader/writer.

15. An applet for enabling a mobile payment device of a user to be updated via an insecure computer network, the mobile payment device storing value and enabling the user to perform cashless transactions with participating merchants, the applet comprising:

a user interface to allow the user to select a transaction type and transaction amount for a transaction;

a server communications module to communicate with an authentication server for authenticating the mobile payment device; and

a device communications module to interface with a reader device to read and update the mobile payment device;

the server communications module facilitating authentication by: receiving an encrypted first message from the authentication server to be decrypted by the mobile payment device, and receiving an encrypted fourth message based on the second message from the authentication server to be decrypted by the mobile payment device;

the device communications module facilitating authentication by: transmitting an encrypted second message from the mobile payment device to the authentication server to be decrypted by the authentication server; transmitting an encrypted third message based on the first message from the mobile payment device to the authentication server, to be decrypted by the authentication server;

wherein the first message is compared with the third message and the second message is compared with the fourth message, where if they match, the identity of the mobile payment device and the authentication server are authenticated with each other to enable the reader device to update the mobile payment device in accordance with the transaction, and the applet downloadable to a client terminal of the user upon authentication.

16. The applet according to claim 15, wherein the applet is a signed Java applet downloadable to a client terminal of the user.