SYSTEM, METHOD AND COMPUTER PROGRAM ARRANGED TO FACILITATE A TRANSACTION

TECHNICAL FIELD

[0001] The present invention relates to a system, method and computer program arranged to facilitate a transaction. Embodiments of the invention find particular, but not exclusive, use in the field of electronic financial transactions, such as e-commerce, EDI (electronic data interchange), web-enabled and electronic point of sale transactions.

BACKGROUND ART

[0002] Nowadays, it is quite common to purchase goods and/or services over the Internet, through 'e-commerce' websites and web-enabled virtual stores. Correspondingly, there has been a need to develop electronic payment systems that facilitate the electronic transfer of value, while maintaining a high level of security.

[0003] One example of a transaction system and method which facilitates secure electronic transactions is described and defined in PCT application PCT/SG2010/000222 (publication number WO 2010/147559), which is incorporated herein by reference.

[0004] WO2010/147559 describes a system and method which allows a user or provider of a 'smart card' to change the state of a transaction channel. That is, the system and method allows a user or provider to 'lock' and/or 'unlock' certain transaction modes, such as web purchasing, point of sale purchasing, etc with respect to other transaction modes.

[0005] Such a system allows a user or provider to 'choose' what types of channels may be used to effect transactions. So, for example, a user may decide that, for security reasons, they will 'lock' their card to prevent the card from being used for web-based purchases, but will leave the card unlocked for traditional point of sale (POS) purchases. If the user's card is stolen, an unauthorized user would not be able

to use the card to effect any web-based purchases, thereby providing an extra level of security.

[0006] In the abovementioned system, which is described herein below in more detail merely to provide some context for the inventive concept described in the specification as a whole, the card has a default setting, that 'locks' the card to prevent web-based purchases.

[0007] Thus, the card lock-unlock feature was developed with a view to provide a user with a mechanism to explicitly 'unlock' the card for web-based purchases. To save the user the effort of having to re-lock the channel after use, the channel may be automatically locked after a web purchase is made, or after a predefined period of time has passed (e.g. 30 minutes).

[0008] One commercially available embodiment provides a timer that is set immediately after the 'Unlock Card' transaction is processed. An incoming purchase transaction immediately re-locks the card and stops the timer. If the timer is not stopped and expires with no web purchase transaction seen, the system locks the card. This feature assists in mitigating web purchase fraud.

[0009] However, while the invention described and defined in WO2010/147559 provides a number of advantages over the prior art, there is a need to provide a more efficient method of locking/unlocking smart cards. In addition, there is also a need to avail card issuers with the locking/unlocking feature from a card network perspective.

[0010] The preceding discussion of the background art is intended to facilitate an understanding of the present invention only. The discussion is not an acknowledgement or admission that any of the material referred to is or was part of the common general knowledge as at the priority date of the application.

SUMMARY OF INVENTION

[0011] In accordance with a first aspect of the invention there is provided a computing device for facilitating transactions between one or more remote devices, comprising a processing module arranged to interact with the one or more remote devices via a communications network and a database arranged to contain

information regarding the state of one or more transaction channels in relation to an account, wherein the processing module is arranged to receive instructions via the communications network from the one or more remote devices and provide information regarding the state of the one or more transaction channels.

[0012] Preferably, the database utilises the Lightweight Directory Access Protocol (LDAP).

[0013] Preferably, the processing module is an intermediary stand-in host arranged to receive instructions from at least one card issuer. In one embodiment the at least one card issuer is a telecommunications operator.

[0014] Alternatively, the processing module is an intermediary stand-in host arranged to receive instructions from at least one card acquirer.

[0015] Preferably, the database is updated via the communications network on a periodic basis.

[0016] Preferably, the processing module is further operable to receive request to change the state of an at least one relatively unsecured transaction channel of the one or more transaction channels from a first state to a second state.

[0017] Preferably in the first state a subsequent transaction message identified with the relatively unsecured transaction channel will be refused and in the second state the transaction message will be passed on for further processing.

[0018] In accordance with a second aspect of the invention there is provided a system arranged to interact with the one or more remote devices via a communications network comprising a server including a database arranged to contain information regarding the state of one or more transaction channels in relation to an account, wherein the module is arranged to receive instructions via the communications network from the one or more remote devices and provide information regarding the state of the one or more transaction channels.

[0019] Preferably, the database utilises the Lightweight Directory Access Protocol (LDAP).

[0020] Preferably, the server is an intermediary stand-in host arranged to receive instructions from at least one card issuer. In one embodiment, the at least one card issuer is a telecommunications operator.

[0021] Preferably, the server is an intermediary stand-in host arranged to receive instructions from at least one card acquirer.

[0022] Preferably, the database is updated via the communications network on a periodic basis.

[0023] Preferably, the server is further operable to receive request to change the state of an at least one relatively unsecured transaction channel of the one or more transaction channels from a first state to a second state.

[0024] Preferably in the first state a subsequent transaction message identified with the relatively unsecured transaction channel will be refused and in the second state the transaction message will be passed on for further processing.

[0025] In accordance with a third aspect of the invention there is provided a method for facilitating transactions between one or more remote devices, comprising the steps of, receiving at a server a request to access information regarding the state of one or more transaction channels in relation to an account; and providing the information regarding the state of the one or more transaction channels to the one or more remote devices.

[0026] In accordance with a fourth aspect there is provided a computer program including at least one instruction capable of being executed by a computing system, which implements a method in the third aspect of the invention.

[0027] In accordance with a fifth aspect there is provided a computer readable medium including a computer program in accordance with the fourth aspect of the invention.

[0028] In a sixth aspect, there is provided a data signal including at least one instruction being capable of being received and interpreted by a computing system, wherein the one instruction implements a method in accordance with the third aspect of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] Further features of the present invention are more fully described in the following description of several non-limiting embodiments thereof. This description is included solely for the purposes of exemplifying the present invention. It should not be understood as a restriction on the broad summary, disclosure or description of the invention as set out above. The description will be made with reference to the accompanying drawings in which:

Figure 1 is an example computing system which is capable of operating a system, method and/or computer program in accordance with an embodiment of the present invention;

Figure 2 is an example network incorporating a computing system in accordance with an embodiment of the present invention; and

Figures 3a to 3c are flow charts depicting process flows in accordance with the method steps of an embodiment of the present invention.

DESCRIPTION OF EMBODIMENTS

[0030] Referring to Figure 1, there is shown an example computing system which is capable of facilitating transactions in accordance with an embodiment of the present invention.

[0031] In Figure 1 there is shown a schematic diagram of a computing system, which in this embodiment is a server 100 suitable for use with an embodiment of the present invention. The server 100 may be used to execute application and/or system services such as a system and method for facilitating an electronic financial transaction in accordance with an embodiment of the present invention.

[0032] With reference to Figure 1, the server 100 may comprise suitable components necessary to receive, store and execute appropriate computer instructions. The components may include a processor 102, read only memory (ROM) 104, random access memory (RAM) 106, an input/output devices such as disc drives 108, input devices 110 (such as an Ethernet port, a USB port, etc.), display 112 such as a liquid crystal display, a light emitting display or any other suitable display and one or more communications link(s) 114.

[0033] The server 100 includes instructions that may be installed in ROM 104, RAM 106 or disc drives 108 and may be executed by the processor 102. There may be provided a plurality of communication links 114 which may variously connect to one or more computing devices such as servers, personal computers, terminals, wireless or handheld computing devices, or mobile communication devices such as a mobile (cell) telephone. At least one of a plurality of communications link may be connected to an external computing network through a telecommunications network.

[0034] In one particular embodiment the device may include a database which may reside on the input output storage device 108. It will be understood that the database may reside on any suitable storage device, which may encompass solid state drives, hard disc drives, optical drives or magnetic tape drives. The database may reside on a single physical storage device or may be spread across multiple storage devices.

[0035] The server 100 includes a suitable operating system 116 which may also reside on a storage device or in the ROM of the server 100. The operating system 116 is arranged to interact with the database and with one or more computer programs to cause the server to carry out the steps, functions and/or procedures in accordance with the embodiments of the invention described herein.

[0036] Figure 2 provides a detailed view of an example of a card network (200) within a wider communications network 202, within which server 100 resides. Server 100 operates as a 'Stand-In' Host as will be described herein below.

[0037] The card network 200 comprises a database 204, which is labeled 'Card Locks Directory Service'. The Card Network is a network such as the MasterCard® or Visa® network, comprising links to relevant financial institutions and routes card transactions from Acquirer to Issuer.

[0038] In more detail, the Stand-In Host 100 operates as an intermediary server operated by a Card Network 200 which "stands in" for a Card issuer and serves to both maintain a collective 'Card Locks Table', which is accessible/controllable by the Card Issuers, and implement 'Card Lock-Unlock' functionality using the 'Card Locks Table' for reference. The Card Locks Directory Service 204 is a directory service that acts as a database and contains a single 'Card Locks Table'. The directory service 204 is preferably implemented using LDAP (Lightweight Directory Access Protocol) instead of a general RDBMS (Relational Database Management System).

[0039] The diagram of Figure 2 further depicts the general operating environment in which embodiment of the invention operates. The components which make up the general operating environment include:

[0040] Telco Network 206 - a network including one or more computing systems which routes m-commerce financial transactions from a computer device such as for example a mobile (cell) phone to the correct Card issuer network;

[0041] Card Issuer Network 208 - a network including one or more computing systems which processes card transactions (such as 'Balance Inquiry' and 'Purchase'), which are forwarded by the Acquirer network via the Card Network;

[0042] Card Acquirer Network 210 - a server which receives card transactions coming from different channels (POS Terminal, ATM Terminal, web) and forwards the transactions to respective Card issuers; and

[0043] General Internet 214 – a user interacts through a browser that links them to the Internet to effect a purchase. In purchasing over the Internet, the user will use their Smart Card (216). Smart Card 216 is at least capable of performing transactions such as (but not including) credit/debit functionalities similar to credit/debit cards.

[0044] The use and operation of the Internet, computers and servers using software applications and payment portals are well known to persons skilled in the art and need not be described in any further detail herein except as is relevant to the present invention.

[0045] The card network 200 will be described in the context of a system that facilitates transactions via the locking/unlocking of smart card 216. The system is known as 'card-network enforced card Lock-Unlock' system.

[0046] **SETTING UP AND USING THE STAND-IN HOST DATABASE**

[0047] The "Card-Network enforced Card Lock-Unlock" system operates through the use of three processes or methodologies: Card Locks Provisioning, Card Locks Setup, and Card Locks Usage.

[0048] In the Card Locks Provisioning process, a record of the Card Account is created within the database (the Card Locks Directory Service) 204 in the Stand-In Host 100, so that a card issuer may interact with the Card Network and cause the card to be locked or unlocked. Once a record of the Card Account has been created in the Card Locks Directory Service 204, the Card Locks can be set up (i.e. the user's or Card Issuer's preferences can be loaded into the Card Locks Directory Service).

[0049] Thereafter, the user can connect to the Card Network (usually through the Card Issuer Network) to lock or unlock the card. The processes within each phase are described in more detail below with reference to Figures 3a to 3c.

[0050] Card Locks Provisioning – Figure 3a

[0051] 1. Provisioning begins with the issuer Card Host sending a 'Create Card Account' request to the Card Network (step 300). It will be understood that this step encompasses sending multiple 'Create Card Account' transactions (i.e. a 'batching' process) for efficiency. As an alternative to batch processing, single 'create card account' requests or transactions may also be sent for purpose of account creation errors to be addressed as it happens. Single 'create card account' requests are useful where network connections is/are unstable and in situations where the protocol used (example ISO 8583) is request-response based and therefore does not support batch file transfer. Single 'create card account' requests also allow account creation errors to be addressed as it happens.

[0052] 2. Stand-In Host 100 adds the request entry in the directory service 'Card locks Table' (step 302).

[0053] 3. The Card Network's Stand-In Host receives the 'Create Card Account' transaction request and performs a LDAP 'Add Entry' operation to create a 'Card Locks' record in the directory service 'Card locks Table' (step 304). For example, if the Card Issuer's default card locks setting is "Allow all transactions except 'ATM Withdrawal' and 'Web Purchase'" then the LDAP entry would be:

dn: 5577510998569107

txnLock: ATMWITHD, WEBPURCH

[0054] where the 'dn' (Distinguished Name) is the Card No. and the custom attribute 'txnLock' lists the transactions, in a comma-delimited format, for which the card is locked.

[0055] Card Locks Setup - Figure 3b

[0056] 1. Once the Stand-In Host has an entry for the account for a Cardholder, the Cardholder can use their m-commerce-enabled computer device such as a mobile (cell) phone to send a 'Card Lock/Unlock' transaction to the Stand-In Host (step 310).

[0057] 2. The Telco Financial Switch routes the transaction to the correct Card issuer (step 312).

[0058] 3. The Card issuer forwards the transaction to the Card Network (step 314). It will be understood that in the embodiment described herein, it is not necessary for the Card Issuer to track the Card Locks setting of each customer - these settings are maintained at the Card Network side.

[0059] 4. The Card Network's Stand-In Host performs a LDAP "Modify Entry" operation to set the Cardholder's card locks accordingly (step 316). For example, if the Cardholder issued a 'Card Lock/Unlock' transaction which unlocked his card for all 'Web Purchase' transactions, the LDAP entry would be modified from:

dn: 5577510998569107

txnLock: ATIVIWITHD, WEBPURCH

[0060] to only:

dn: 5577510998569107

txnLock: ATNIWITHD

[0061] 5. Subsequently, the Stand-In Host performs a 'Card Lock/Unlock' procedure (detailed in PCT/SG2010/000222) (step 318). For example, the Stand-In Host creates a Timer that expires in for example, 15 minutes. Once the Timer expires, the 'Web Purchase' lock is restored in the LDAP entry via a LDAP 'Modify Entry' operation, if it has not already been restored (by the Stand-In Host in the event that a 'Web Purchase' transaction was received within the 15-minute window).

[0062] Card Locks Usage – Figure 3c

[0063] Usage occurs either when the Cardholder issues a transaction such as a 'Web Purchase' transaction on their explicitly unlocked card, or when an unauthorized user issues a similar transaction on the locked card. In either case, the Card Acquirer receives the transaction from the Merchant, and forwards it to the Card Network.

[0064] 1. The Card Networks Stand-In Host performs a LDAP 'Search Entry' request on the Card Locks Directory Service and retrieves the cardholder's locks record (step 320).

[0065] 2. Subsequently, the Stand-In Host performs "Card lock-unlock" procedures (lock-unlock procedure detailed in PCT/SG2010/000222) (step 322). In more detail, the Stand-In Host checks the cardholders 'Card Locks' record. If the card is not locked for the particular transaction type, then the transaction is freely forwarded to the Card Issuer for processing. The Stand-In Host then restores the transaction lock in the Card Locks Directory Service (via a LDAP 'Modify Entry' operation), since the transaction has been performed. However, if the card is locked for the particular transaction type, then the Stand-In Host immediately declines the transaction, and does not forward the transaction to the Card issuer.

[0066] 3. The Card Network returns the Approved or Declined response to the Card Acquirer (step 324).

[0067] 4. The Card Acquirer passes on the response to the originating channel, which notifies the user on the result of his transaction (step 326).

[0068] ADVANTAGES

[0069] The 'Card-Network-enforced Card Lock-Unlock', provides a number of advantages over prior art systems. As the system operates from a central server (i.e. the Stand-In Host), there is no need for each card issuer to maintain a separate server for card lock-unlock data. Appropriate information can be sent to the Stand-In Host from all card issuers.

[0070] Correspondingly, as card issuers are not required to maintain individual Stand-In Hosts, more card issuers are likely to use the Stand-In Host, which in turn increases amenity to end users while allowing card issuers to offer the service to their clients without having to set up and maintain an intermediary (or additional) server. To provide the card network with a Stand-In Host assists in popularizing the service and establishing a de-facto standard worthy of a card industry-agreed ISO 8583 (or similar industry standard) response code for the 'Card is locked' condition (as explained below).

[0071] Importantly, the system provides a shorter transaction response time to card acquirers when the card is locked, since the card network need not forward certain transactions to the card issuer.

[0072] As mentioned above, the development of card network-enforced Stand-In Host allows for the development of a standard ISO 8583 response code for the 'Card is locked' condition. Currently, as implemented in one existing commercial embodiment of the prior art, when the card is locked and a web purchase transaction occurs, the card issuer's host blocks the transaction as expected. However, as there is no current industry standard for response codes related to card locks, the error notification message displayed by the merchant website is often vague, e.g., "Your card could not be authorized."

[0073] By providing the card network with the means to enforce the feature, the card network, which caters to hundreds of card issuers, is able to use the card lock-unlock feature across the entire network (i.e. to all card providers and users) thereby justifying the creation of a particular ISO 8583 response code for the 'Card is locked' condition.

[0074] Advantageously, utilizing a Stand-In Host allows a uniform 'card lock-unlock' service to be provided to all card issuer clients. If no industry-standard ISO 8583 response code for the 'Card is locked' condition is available, the card network could assign one code for use by all card issuers, assuring that all of its card acquirers would receive the same response code consistently when the condition occurs.

[0075] Once the response code is established, merchant websites would be able to provide much clearer error messages, such as "The transaction could not be processed because your card is locked. Please unlock your card and repeat the payment action."

[0076] Moreover, in one embodiment, the 'Card Locks Table' is implemented using a lightweight directory service (such as LDAP) instead of a relational database. Maintaining and operating the 'Card Locks Table' requires only a directory service with basic CRUD (Create, Read, Update, and Delete) operations. There are no SQL JOIN operations required since only one table is used. As such, information can be saved and retrieved very efficiently and quickly from the Stand-In Host, which ensures that there is no appreciable delay in a transaction being authorized or declined, and also in a card being locked or un-locked. In other words, the Stand-In Host is almost completely transparent to the Card Issuer, the Card Acquirer and the user (customer).

[0077] Moreover, as all 'decline' responses are recorded in a central location, it is possible to form a bird's-eye view of which card issuer has the most number of "Card is locked" decline responses. This collection of data is useful to security specialists looking for trends in web purchase fraud.

[0078] **VARIATIONS AND MODIFICATIONS**

[0079] Although not required, the embodiments described with reference to the figures can be implemented via an application programming interface (API) or as a series of libraries, for use by a developer, and can be included within another software application, such as a terminal or personal computer operating system or a portable computing device operating system, or within a transaction processing system.

[0080] Generally, as program modules include routines, programs, objects, components and data files that perform or assist in the performance of particular functions, it will be understood that the functionality of the software application may be distributed across a number of routines, programs, objects or components to achieve the same functionality as the embodiment and the broader invention claimed herein. Such variations and modifications are within the purview of those skilled in the art.

[0081] It will also be appreciated that where methods and systems of the present invention and/or embodiments are implemented by computing systems or partly implemented by computing systems then any appropriate computing system architecture may be utilized. This includes standalone computers, network computers and dedicated computing devices (such as hardware-based arrays).

[0082] Where the terms “computer”, "computing system" and "computing device" are used in the specification, these terms are intended to cover any appropriate arrangement of computer hardware for implementing the inventive concept and/or embodiments described herein.

CLAIMS:

1. A computing device for facilitating transactions between one or more remote devices, comprising

a processing module arranged to interact with the one or more remote devices via a communications network and a database arranged to contain information regarding the state of one or more transaction channels in relation to an account, wherein the processing module is arranged to receive instructions via the communications network from the one or more remote devices and provide information regarding the state of the one or more transaction channels.

2. A computing device in accordance with claim 1, wherein the database utilises the Lightweight Directory Access Protocol (LDAP).

3. A computer device in accordance with claim 1, wherein the processing module is an intermediary stand-in host arranged to receive instructions from at least one card issuer.

4. A computer device in accordance with claim 3, wherein the at least one card issuer is a telecommunications operator.

5. A computer device in accordance with claim 1, wherein the processing module is an intermediary stand-in host arranged to receive instructions from at least one card acquirer.

6. A computing device in accordance with claim 1 or claim 2, wherein the database is updated via the communications network on a periodic basis.

7. A computer device according to claim 3, wherein the processing module is further operable to receive request to change the state of an at least one relatively unsecured transaction channel of the one or more transaction channels from a first state to a second state.

8. A system arranged to interact with the one or more remote devices via a communications network comprising a server including a database arranged to contain information regarding the state of one or more transaction channels in relation to an account, wherein the module is arranged to receive instructions via the communications network from the one or more remote devices and provide information regarding the state of the one or more transaction channels.

9. A system in accordance with claim 8, wherein the database utilises the Lightweight Directory Access Protocol (LDAP).

10. A system in accordance with claim 8, wherein the server is an intermediary stand-in host arranged to receive instructions from at least one card issuer.

11.A system in accordance with claim 10, wherein the at least one card issuer is a telecommunications operator.

12. A system in accordance with claim 8, wherein the server is an intermediary stand-in host arranged to receive instructions from at least one card acquirer.

13.A system in accordance with claim 8 or claim 9, wherein the database is updated via the communications network on a periodic basis.

14.A system in accordance with claim 10, wherein the server is further operable to receive request to change the state of the at least one relatively unsecured transaction channel of the one or more transaction channels from a first state to a second state.

15.A method for facilitating transactions between one or more remote devices, comprising the steps of, a. receiving at a server a request to access information regarding the state of one or more transaction channels in relation to an account; and providing the information regarding the state of the one or more transaction channels to the one or more remote devices.

16.A computer program, including at least one instruction capable of being executed by a computing system, which implements a method in accordance with claim 15.

17.A computer readable medium including a computer program in accordance with claim 16.