METHOD FOR CREATING AND DISCARDING DYNAMIC VIRTUAL CARD

TECHNICAL FIELD

[0001] The present invention relates to a method of creating and discarding a dynamic virtual card, which provides a card provided as hardware as a virtual card and dynamically creates and discards the virtual card. The present invention particularly relates to a method for distributing a virtual card platform for a dynamic virtual card to a server and a mobile device.

BACKGROUND ART

[0002] Mobile cards have been used for the purpose of traffic card, payment of goods/services, identification, and accumulation/use of points. For cards that are generally used as payment methods, independent security devices (e.g., USIM, IC Chip) for the purpose of preventing theft through modulations or duplication are used.

[0003] FIG. 1 is a view for explaining a conventional mobile card service.

[0004] An independent security device (e.g., USIM, IC chip, H / W Secure Element-Based Card) may be divided into a layer of a card platform 12 (Chip Operating System) for performing a security role and an application management role as an operating system of the security device and a layer of a payment application 11 (payment App) for storing payment information and performing a payment transaction with a payment terminal 20 (=

charge/payment device). The payment application 11 executed in the card platform 12 of the security device 10 is generally secured.

[0005] According to existing mobile card services, the security device 10 may be installed in a mobile device such as a smart phone. The mobile device and the security device may be operated by an operating system that is different from each other, and the mobile device and the security device may be provided with separate user applications.

[0006] According to the existing mobile card service, a payment application 11 is installed in the security device 10 mounted on the mobile device, and a transaction may be made through a process of transmitting data stored locally in the payment application 11 and a transaction authentication code calculated through a security key to a terminal application.

[0007] That is, the payment application 11 may receive the financial card by receiving and storing static data from a payment management server (not shown) existing on the network. Upon receiving a transaction request from the payment terminal 20, the payment application 11 performs a transaction using the stored static data, and stores the transaction history information in the storage of the payment application 11 as needed, so that the issued financial card may be used. At this time, the issued payment application 11 may be used for payment or charging transactions in an offline mode that is not connected to the payment management server.

[0008] There are the following problems in the case where the payment application 11

is installed in the above-described physical security device 10 and used as a card medium.

[0009] First, a payment application is installed in a card to which an independent security device is applied, for example, an IC card, and in order to store the payment information in the installed payment application, typically, there must be a business agreement between the IC card holder (e.g., a carrier) and the payment application provider. And, the payment application provider must be entrusted with the technical authority of the physical security device from the owner of the IC card. In spreading the service provided by the payment application provider, such a business agreement procedure has a business problem that it is inevitably dependent on the IC card holder (communication company) for business.

[0010] Also, since the physical security device has a small memory space, the types of applications that may be installed may be limited.

[0011] Also, the physical security device has a structure without network function on its own. Therefore, as described above, since the once issued payment application is used for offline payment or charge transactions that are not associated with the payment management server, it is difficult to control a lost or stolen IC card. That is, a lost or stolen IC card may be used independently without control of the management server, there is a risk of being stolen.

DISCLOSURE OF THE INVENTION

TECHNICAL PROBLEM

[0012] In order to solve the above-mentioned problems, the present invention provides a dynamic virtual card creation method capable of controlling theft prevention, application management, and loss/theft so that the use of an independent security medium is not required.

[0013] Specifically, a method for distributing and installing a dynamic virtual card platform including a plurality of function modules using a plurality of devices (ex: server and mobile terminal) capable of mutual communication is provided. That is, provided is a method of dynamically creating and discarding a dynamic virtual card platform to be effectively operated in a mobile device in a separate server, and accordingly thereto, determining whether the server and the mobile device are organically valid, and when a dynamic card platform is created between the mobile device and the server, driving a card application or discarding a dynamically created platform.

TECHNICAL SOLUTION

[0014] According to an embodiment of the present invention, a method for distributively installing a dynamic virtual card platform including a plurality of function modules using a plurality of devices capable of mutual communication includes: a platform updating step of updating, by a first device, a first function module constituting a valid dynamic virtual card platform that operates valid and a second function module associated with the first function module; and a platform distribution and installation step of storing,

by the first device, the updated first function module in the first device and providing only the second function module of the first function module and the second function module to a remote security module.

[0015] The first function module may include an ISD module and the second function module includes an APSD module.

[0016] The method may further include, before the platform updating step, receiving, by the first device, a request for financial payment preparation from a third device, wherein the platform updating step may be performed each time the request is received, and the third device and the security module may be capable of communicating with each other.

[0017] The first device may be a server and the security module may be a security device capable of communicating with the third device or a module implemented by software in the third device, wherein in the platform distribution and installation step, the second function module may be provided to the security module using wire communication or wireless communication between the first device and the third device.

[0018] According to an embodiment of the present invention, a virtual card creation method for dynamically creating a virtual card using a plurality of devices capable of mutual communication includes: a platform updating step of updating, by a first device, a first function module constituting a valid dynamic virtual card platform that operates valid and a second function module associated with the first function module; a platform distribution and installation step of storing, by the first device, the updated first function

module in the first device and providing only the second function module of the first function module and the second function module to a remote security module; a payment application updating step of updating, by the first device, a value storage module constituting a dynamic virtual payment application that operates in the dynamic virtual card platform and a relay module associated with the value storage module; and a payment application distribution and installation step of storing, by the first device, the updated value storage module only in the first device and providing the updated relay module to the security module, wherein the relay module is configured to perform a function of relaying a payment transaction using a financial value stored in the value storage module by a third device communicating with the security module.

[0019] When the payment transaction is performed, in order to invalidate the updated dynamic virtual card platform and the virtual card defined by the updated payment application, when the payment transaction is performed, the updated dynamic virtual card platform may be configured to be invalidated.

[0020] The method may further include receiving, by the first device, a request for financial payment preparation from the third device before the platform updating step and the payment application updating step, wherein the platform updating step and the payment application updating step may be performed each time the request is received.

[0021] The payment application updating step may include: dividing the updated relay module into a plurality of segments; creating a digital signature value from the plurality of

segments; encrypting the plurality of segments using one or more keys; and scrambling the plurality of encrypted segments, wherein the payment application distribution and installation step may include providing the scrambled information to the security module, and the one or more keys and the digital signature value may be provided to the security module.

[0022] The security module may be configured to perform: descrambling the scrambled information; decrypting the descrambled information using the one or more keys; verifying the decrypted information using the digital signature value; and installing the relay module in the security module using the verified decrypted information.

[0023] According to an embodiment of the present invention, a server for distributively installing a dynamic virtual card platform including a plurality of functional modules using a plurality of devices capable of mutual communication, wherein the server is to perform a platform updating step of updating a first function module constituting a valid dynamic virtual card platform that operates valid and a second function module associated with the first function module, and to perform a platform distribution and installation step of storing the updated first function module in the server and providing only the second function module of the first function module and the second function module to a remote security module.

[0024] The first function module may include an ISD module and the second function module may include an APSD module.

[0025] The server may further perform, before the platform updating step, receiving, by the server, a request for financial payment preparation from a third device, wherein the platform updating step may be performed each time the request is received, and the third device and the security module may be capable of communicating with each other.

ADVANTAGEOUS EFFECTS

[0026] According to the present invention, a dynamic virtual card platform may be distributed and provided to a server and a user portable device capable of communicating with the server. Accordingly, a dynamic virtual card using a server (=cloud) based dynamic virtual card platform may be provided. By controlling the dynamic virtual card in real time, the card may be prevented from being modulated, duplicated, or hijacked.

[0027] In addition, through the present invention, an application installed in the dynamic virtual card platform may be easily managed, and applications of various purposes may be easily installed.

[0028] In addition, application data for the dynamic virtual card may be freely updated through the network. In addition, the dependency between the owner of the physical security device and the provider of the application installed in the dynamic virtual card platform may be eliminated.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] FIG. 1 is a view for explaining a conventional mobile card service.

[0030] FIG. 2 is a view illustrating a mobile card service according to an embodiment of the present invention.

[0031] FIG. 3 is a flowchart illustrating a mobile card service according to an embodiment of the present invention.

[0032] FIG. 4 is a view embodying the embodiment of FIG. 3.

[0033] FIG. 5 is a flowchart illustrating steps performed after updating a relay module in a cloud server according to an embodiment of the present invention.

[0034] FIG. 6 is a flowchart illustrating a process performed when a relay module is received in a mobile device according to an embodiment of the present invention.

MODE FOR CARRYING OUT THE INVENTION

[0035] Hereinafter, embodiments of the present invention will be described with reference to the accompanying drawings. However, the present invention is not limited to the embodiments described herein, but may be implemented in various other forms. The terminology used herein is for the purpose of understanding the embodiments and is not intended to limit the scope of the present invention. In addition, the singular forms used below include plural forms unless the phrases expressly have the opposite meaning.

[0036] FIG. 2 is a view illustrating a mobile card service according to an embodiment

of the present invention.

[0037] Here, the mobile card service may be a service for providing a financial card to a mobile device such as a smart phone virtually and for charging/paying using the financial card in cooperation with the financial card and the mobile device. At this time, the mobile device starts a request for a financial activity to another one of the charge/payment devices, and the other responds to the request, so that the mobile card service may be performed.

[0038] A system for providing a mobile card service according to an embodiment of the present invention may include a charge/payment device 20, a cloud server 30, and a mobile device 40.

[0039] At this time, the mobile device 40 may include an operating system for the mobile device 40 and a UX/UI application 41 running on the operating system.

[0040] The mobile device 40 may have a security module 42 installed therein.

[0041] At this time, the mobile device 40 and the security module 42 may be independent computing devices. In this case, the security module may be provided using a conventional Secure Element (SE).

[0042] Or, the security module 42 may be a module that runs as software in the mobile device 40.

[0043] The UX/UI application 41 may be, for example, an application that a user of the mobile device 40 uses to actually make a payment through the mobile device.

[0044] The payment application 11 and the card platform 12 described with reference

to FIG. 1 may be distributed and placed in the cloud server 30 and the security module 42 as shown in FIG. 2. That is, if the payment application 11 is conventionally installed only in the security module 42, in contrast, in the present invention, the payment application 11 may be divided into the value storage module 32 and the relay module 52 in the cloud server 30 and the security module 42, respectively.

[0045] According to the present invention, since the conventional card platform is divided and installed in a plurality of devices (server and mobile device) through the network, the card platform according to the present invention may be referred to as a 'dynamic virtual card platform'. In one embodiment of the present invention, since the dynamic virtual card platform may be updated at each financial transaction request, it may be referred to as a 'dynamic virtual card platform'.

[0046] Also, if the card platform 12 is conventionally installed only in the security module 42, in contrast, in the present invention, the dynamic virtual card platform 12 is decomposed into a first function module 31 and a second function module 51. The first function module 31 and the second function module 51 may be distributively installed in the cloud server 30 and the security module 42, respectively.

[0047] The dynamic virtual card 1 may be a combination of the payment application 11 and the dynamic virtual card platform 12. According to the present invention, since the payment application 11 is divided and installed in a plurality of devices (server and mobile device) through the network, the payment application according to the present invention

may be referred to as a ‘dynamic virtual payment application’. Since the dynamic virtual payment application may be updated whenever there is a financial transaction request in one embodiment of the present invention, it may also be referred to as a 'dynamic virtual payment application'.

[0048] In the embodiment of FIG. 2, the cloud server 30 and the mobile device 40 may be connected to each other through a network to exchange information.

[0049] When the payment is made through the charge/payment device 20, payment may be made using the value storage module 31 stored in the cloud server 30. At this time, the relay module 51 may perform a function of relaying the payment transaction with the charge/payment device 20 using the financial value stored in the value storage module 31.

[0050] At this time, the mobile device 40 may be implemented to help data exchange between the security module 42 and the cloud server 30, and help data exchange between the charge/payment device 20 and the security module, and this role may be implemented by the UX/UI APP 41. For example, the UX/UI APP 41 may be provided by the person providing the dynamic virtual payment application 11.

[0051] The actual financial transaction is performed between the dynamic virtual card 1 and the charge/payment device 20, and the mobile device 40 may provide a communication function for the financial transaction.

[0052] In this case, the first function module 32 may include, for example, an Issuer Security Domain (ISD) and the second function module 52 may include, for example, an

Application Provider Security Domain (APSD), a Certificate Authority Security Domain (CASD), and a User Authentication Framework (UAF).

[0053] FIG. 3 is a flowchart illustrating a mobile card service according to an embodiment of the present invention.

[0054] In step S10, the UI application 41 of the mobile device 40 may request the financial server to prepare a financial payment. Various functions of the UI application 41 may be activated by the user of the mobile device 40 through the user interface of the mobile device 40.

[0055] The financial payment preparation request may be triggered, for example, by a user of the mobile device 40 accessing the charge/payment device 20 through the action of activating the UI application 41 for financial payment.

[0056] In step S20, in the cloud server 40, the first function module constituting the valid dynamic virtual card platform 12 and the second function module associated with the first function module may be updated. When the first function module and the second function module are updated, the dynamic virtual card platform 12 defined by the first function module and the second function module is updated.

[0057] In this manner, the dynamic virtual card platform 12 may be updated every time the UI application 41 requests the financial payment preparation.

[0058] In step S30, the cloud server 40 may store the updated first function module in the cloud server 30.

[0059] In step S31, the cloud server 40 may transmit the updated second function module to the security module 42 of the mobile device 40 through the wired/wireless network. In this process, the mobile device 40 may provide wired/wireless network communication functions for the security module 42.

[0060] In step S40, the cloud server 40 may update the value storage module 31 constituting the dynamic virtual payment application 11 operating in the dynamic virtual card platform 12 and the relay module 51 associated with the value storage module. For example, the value storage module may be a Cloud Tmoney TM, and the relay module may be a Tmoney Agent TM.

[0061] When the value storage module 31 and the relay module 51 are updated, the dynamic virtual payment application 11 defined by the value storage module 31 and the relay module 51 is updated.

[0062] In this manner, the dynamic virtual payment application 11 may be updated every time the UI application 41 requests the financial payment preparation.

[0063] In step S50, the cloud server 40 may store the updated value storage module 31 in the cloud server 30.

[0064] In step S51, the cloud server 40 may transmit the updated relay module 51 to the security module 42 of the mobile device 40 through the wired/wireless network. In this process, the mobile device 40 may provide wired/wireless network communication functions for the security module 42.

[0065] In step S60, the security module 42 of the mobile device 40 may install the updated and provided relay module 51.

[0066] Now, after the financial payment preparation request is made by the user of the mobile device 40 accessing the charge/payment device 20, for example, when a salesperson operating the charge/payment device 20 controls the charge/payment device 20, so that this causes a financial transaction between the dynamic virtual card and the charge/payment device 20. Or the triggering of the financial transaction may be made by the dynamic virtual card or the UI application or the mobile device 40.

[0067] In step S70, if the financial transaction is triggered, it is possible to verify the consistency between the first function module and the second function module constituting the dynamic virtual card platform 12 and verify the consistency between the value storage module and the relay module constituting the dynamic virtual payment application. The reason for verifying consistency is that each time the card platform and payment application are updated, the corresponding modules with different mapping values are dynamically created in pairs.

[0068] The verification of the consistency may be performed by the cloud server or the dynamic virtual card or the UI application, and for this, communication between the mobile device 40 and the cloud server 30 may be maintained.

[0069] The cloud server may be physically implemented by one server or by a plurality of different devices.

[0070] In step S80, the dynamic virtual card may perform payment between the value storage module and the charge / payment device through the relay module.

[0071] In step S90, if the cloud server 30 confirms that the payment is successfully completed or the payment is failed, the cloud server 30 may remove the updated first function module and value storage module of the cloud server 30.

[0072] In step S91, if the security module 42 confirms that the payment is successfully completed or the payment is failed, the security module 42 may remove the updated second function module and the relay module of the security module 42.

[0073] In one embodiment of the present invention, all the updated modules constituting the dynamic virtual card may be destroyed after the payment transaction process is performed successfully or unsuccessfully. That is, every time the financial payment preparation is requested as in step S10, all the modules constituting the virtual card, that is, the dynamic virtual card, may be updated.

[0074] And, the updated dynamic virtual card may be removed after the payment transaction process is performed once as in step S90 and step S91. The above description may mean that the dynamic virtual card is created dynamically whenever the financial payment preparation is requested (whenever a card is requested to be created), and the dynamic virtual card program is terminated when the transaction ends.

[0075] FIG. 4 is a diagram embodying the embodiment of FIG. 3.

[0076] The cloud server 30 may include a service application server 35, a payment

management unit 36, and a V-Card platform management unit 37.

[0077] The mobile device 40 may include a UI application 41 and a security module 42. The UI application 41 may be configured to select a type of transportation means such as a one-time ticket, a commuter pass, a cloud Tmoney, a Tmoney pay, and a mobile Tmoney. When a user of the mobile device selects a service subscription and/or a desired mode of transportation, the UI application 41 may transmit a service subscription and/or card activation request to the service application server of the cloud server 30.

[0078] When the service application server 35 receives the card activation request, for example, for the Cloud Tmoney, it may request the payment management unit 36 and the V-Card Platform Management 37 to activate the cloud Tmoney. Then, the payment management unit 36 and the V-Card Platform Management 37 may create a dynamic virtual card. At this time, the Cloud Tmoney 31 corresponding to the value storage module and the ISD module of the card platform may be stored in the server, and the Tmoney Agent 51 corresponding to the relay module and the APSD, CASD, and UAF modules of the card platform may be stored in the security module 42 of the mobile device 40. Upon receiving the activation request from the payment management unit 36 and the V-Card Platform Management 37, the payment management unit 36 may create an account and personalize the Tmoney agent. And, the V-Card Platform Management 37 may personalize each security domain (SD) module and UAF module. For each mobile device, the source codes of the Tmoney agent and each of a secure domain (APSD, CASD) module and a

UAF module are different from each other, and may be encrypted and scrambled and transmitted to the security device of the mobile device. In the security device, at the time of application execution, the encrypted and scrambled modules in the memory may be descrambled and decrypted and then used for transactions.

[0079] The cloud Tmoney 31 and the Tmoney agent 51 corresponding to the payment application, and the ISD, APSD, CASD, and UAF corresponding to the card platform may function as one virtual card 1.

[0080] At this time, the account and security information for creating the dynamic virtual card are stored in the cloud server, and ID and non-security information for accessing the account may be stored in the mobile device.

[0081] At this time, payment may be performed through the cloud Tmoney 31 using the Tmoney agent 51.

[0082] FIG. 5 is a flowchart illustrating steps performed after updating a relay module in a cloud server according to an embodiment of the present invention. That is, FIG. 5 is a flowchart showing a process performed between step S40 and step S51 of FIG. 3.

[0083] This will be described below with reference to FIG. 5.

[0084] In step S100, the updated relay module may be divided into a plurality of segments.

[0085] In step S110, the digital signature value may be created using the plurality of segments.

[0086] In step S120, the digital signature value may be created using the plurality of segments.

[0087] In step S130, the plurality of encrypted segments may be scrambled.

[0088] In step S140, the mobile device 40 may transmit the scrambled information, information on the used one or more keys, and the generated digital signature value to the security module 42 of the mobile device 40.

[0089] FIG. 6 is a flowchart illustrating a process performed when a relay module is received in a mobile device according to an embodiment of the present invention. That is, FIG. 6 is a flowchart showing a process performed in step S60 of FIG. 3.

[0090] This will be described below with reference to FIG. 6.

[0091] In step S200, the security device may receive information scrambled from the cloud server, information on one or more keys, and digital signature value.

[0092] In step S210, the scrambled information may be restored to its original arrangement.

[0093] In step S220, the decompressed descrambling information may be decoded using information on the one or more keys.

[0094] In step S230, the information decrypted in step S220 may be verified using a digital signature value.

[0095] In step S240, the relay module may be installed using the verified decrypted information.

[0096] In the present invention, the dynamic virtual card platform described may be an OS for the dynamic virtual card. And, the dynamic virtual payment application may be an application program running on the dynamic virtual card platform.

[0097] It will be apparent to those skilled in the art that various modifications and variations may be made in the present invention without departing from the spirit or essential characteristics thereof. The contents of each claim may be combined with other claims without departing from the scope of the claims.

CLAIMS

1. A method for distributively installing a dynamic virtual card platform including a plurality of function modules using a plurality of devices capable of mutual communication, the method comprising:

a platform updating step of updating, by a first device, a first function module and a second function module associated with the first function module, the first function module and the second function module constituting a dynamic virtual card platform that operates valid; and

a platform distribution and installation step of storing, by the first device, the updated first function module only in the first device and providing the updated second function module to a remote security module.

2. The method of claim 1, wherein the first function module comprises an ISD module and the second function module comprises an APSD module.

3. The method of claim 1, further comprising before the platform updating step, receiving, by the first device, a request for financial payment preparation from a third device,

wherein the platform updating step is performed each time the request is received, and

the third device and the security module are capable of communicating with each other.

4. The method of claim 3, wherein the first device is a server and

the security module is a security device capable of communicating with the third device or a module implemented by software in the third device,

wherein in the platform distribution and installation step, the second function module is provided to the security module using wire communication or wireless communication between the first device and the third device.

5. A virtual card creation method for dynamically creating a virtual card using a plurality of devices capable of mutual communication, the method comprising:

a platform updating step of updating, by a first device, a first function module and a

second function module associated with the first function module, the first function module and the second function module constituting a dynamic virtual card platform that operates valid;

a platform distribution and installation step of storing, by the first device, the updated first function module only in the first device and providing the updated second function module to a remote security module.

a payment application updating step of updating, by the first device, a value storage module constituting a dynamic virtual payment application that operates in the dynamic virtual card platform and a relay module associated with the value storage module; and

a payment application distribution and installation step of storing, by the first device, the updated value storage module only in the first device and providing the updated relay module to the security module,

wherein the relay module is configured to perform a function of relaying a payment transaction using a financial value stored in the value storage module by a third device communicating with the security module.

6. The method of claim 5, wherein when the payment transaction is performed, in order to invalidate the updated dynamic virtual card platform and the virtual card defined by the updated payment application,

when the payment transaction is performed, the updated dynamic virtual card platform is configured to be invalidated.

7. The method of claim 5, further comprising receiving, by the first device, a request for financial payment preparation from the third device before the platform updating step and the payment application updating step,

wherein the platform updating step and the payment application updating step are performed each time the request is received.

8. The method of claim 5, wherein the payment application updating step comprises:

dividing the updated relay module into a plurality of segments;

creating a digital signature value from the plurality of segments;

encrypting the plurality of segments using one or more keys; and

scrambling the plurality of encrypted segments,

wherein the payment application distribution and installation step comprises providing the scrambled information to the security module, and

the one or more keys and the digital signature value are provided to the security module.

9. The method of claim 8, wherein the security module is configured to perform:

descrambling the scrambled information;

decrypting the descrambled information using the one or more keys;

verifying the decrypted information using the digital signature value; and

installing the relay module in the security module using the verified decrypted information.