US 20120149333A1

(19) **United States**

(12) **Patent Application Publication**

Wu et al.

(10) **Pub. No.: US 2012/0149333 A1**

(43) **Pub. Date: Jun. 14, 2012**

(54) **METHOD AND SYSTEM FOR REMOTE CONTROL OF A SMART CARD**

(75) Inventors: **Chuanxi Wu**, Shenzhen (CN); **Jingwang Ma**, Shenzhen (CN)

(73) Assignee: **ZTE CORPORATION**, Shenzhen, Guangdong (CN)

(21) Appl. No.: **13/258,796**

(22) PCT Filed: **Dec. 23, 2009**

(86) PCT No.: **PCT/CN2009/075893**

§ 371 (c)(1), (2), (4) Date: **Feb. 28, 2012**

(30) **Foreign Application Priority Data**

Aug. 28, 2009 (CN) 200910171737.9

Publication Classification

(51) **Int. Cl.**
H04W 12/00 (2009.01)

(52) **U.S. Cl.** **455/411**

(57) **ABSTRACT**

The present application discloses a method and system for remote control of a smart card. The method includes: a smart card management platform receives a request to destroy the smart card from a subscriber (S**101**); according to the request, the smart card management platform performs interactive processing with a terminal side via a mobile network platform to make the terminal side destroy the smart card (S**103**). The present application enables the subscriber to avoid loss when the terminal is robbed, lost, stolen, or is illegally used seriously, and provide a higher flexibility to the payment system.

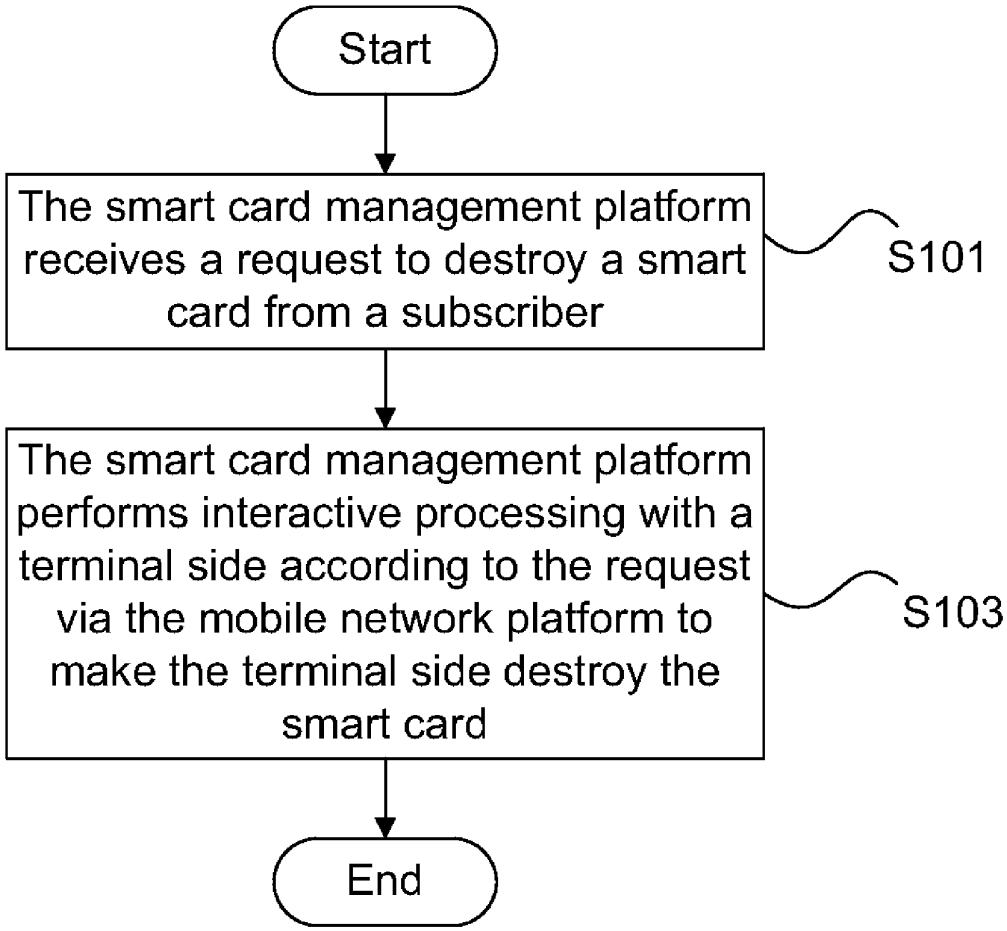


Fig. 1

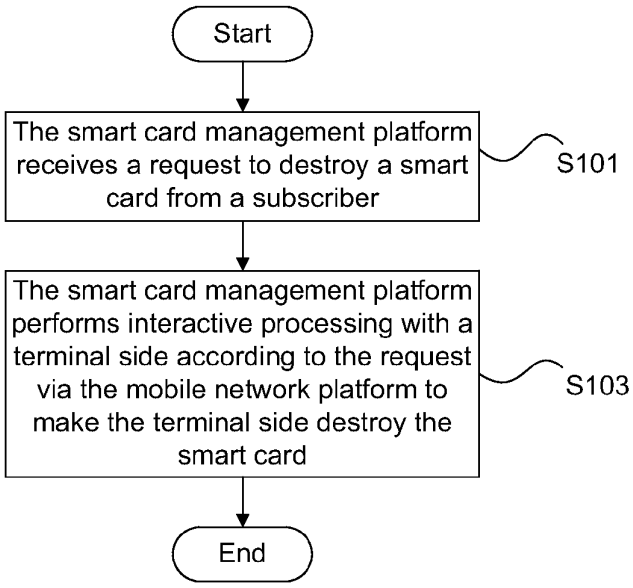

Start
The smart card management platform receives a request to destroy a smart card from a subscriber
S101
The smart card management platform performs interactive processing with a terminal side according to the request via the mobile network platform to make the terminal side destroy the smart card
S103
End

Fig. 2

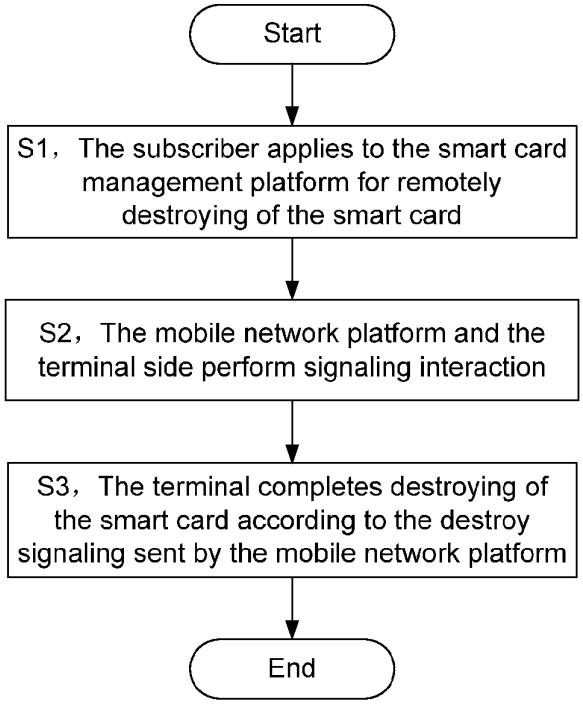

Start
S1, The subscriber applies to the smart card management platform for remotely destroying of the smart card
S2, The mobile network platform and the terminal side perform signaling interaction
S3, The terminal completes destroying of the smart card according to the destroy signaling sent by the mobile network platform
End

Fig. 3

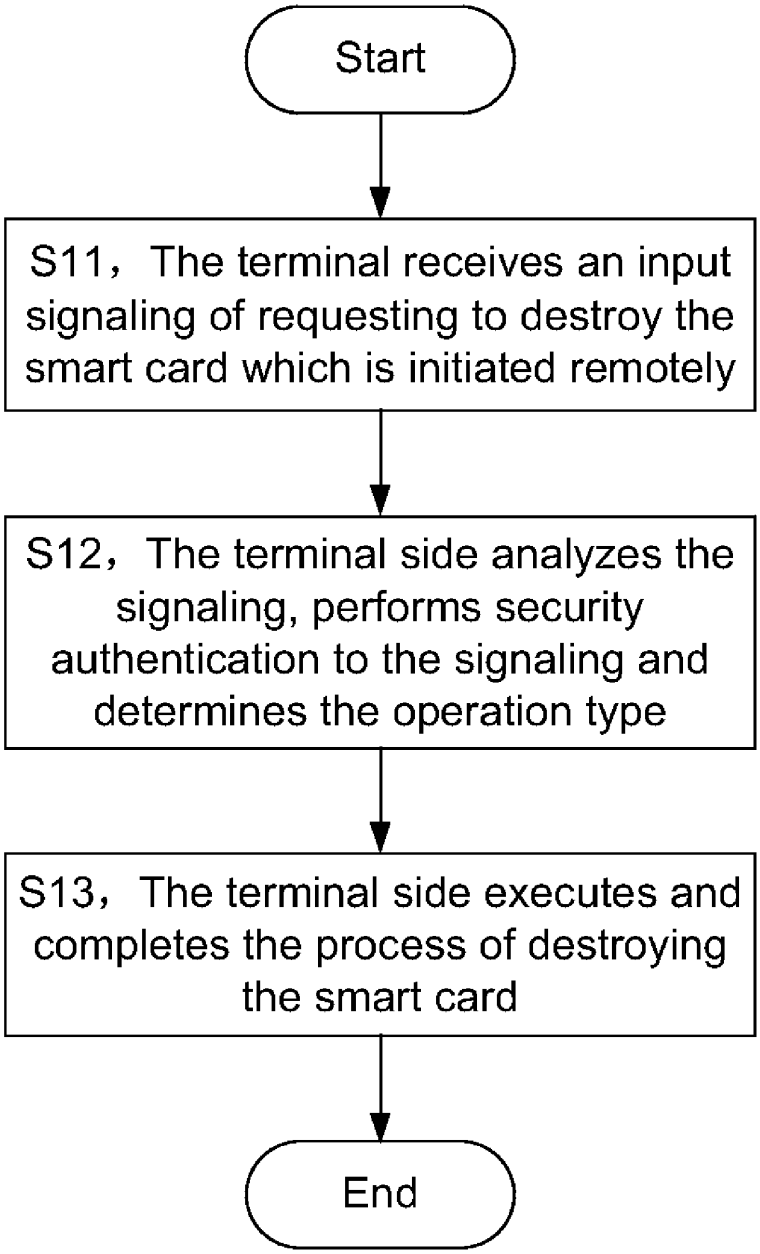

Start
S11，The terminal receives an input signaling of requesting to destroy the smart card which is initiated remotely
S12，The terminal side analyzes the signaling, performs security authentication to the signaling and determines the operation type
S13，The terminal side executes and completes the process of destroying the smart card
End

Fig. 4

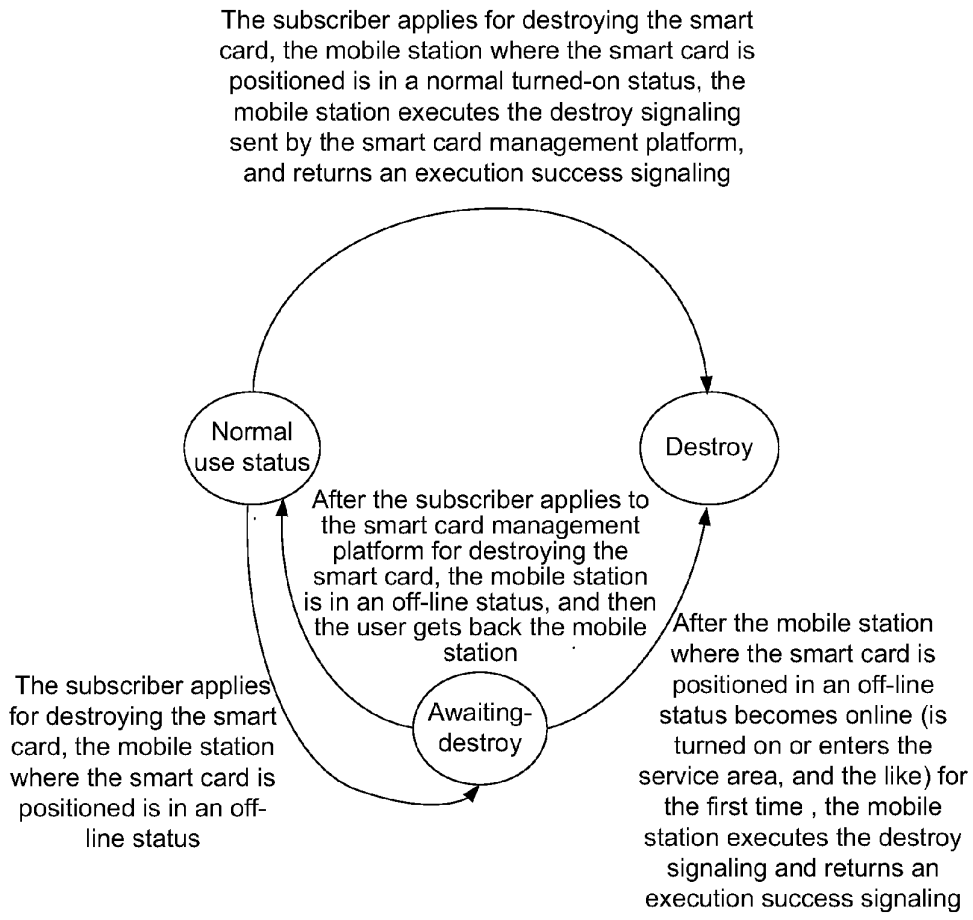

The subscriber applies for destroying the smart card, the mobile station where the smart card is positioned is in a normal turned-on status, the mobile station executes the destroy signaling sent by the smart card management platform, and returns an execution success signaling
Normal use status
Destroy
After the subscriber applies to the smart card management platform for destroying the smart card, the mobile station is in an off-line status, and then the user gets back the mobile station
Awaiting-destroy
The subscriber applies for destroying the smart card, the mobile station where the smart card is positioned is in an off-line status
After the mobile station where the smart card is positioned in an off-line status becomes online (is turned on or enters the service area, and the like) for the first time , the mobile station executes the destroy signaling and returns an execution success signaling

Fig. 5

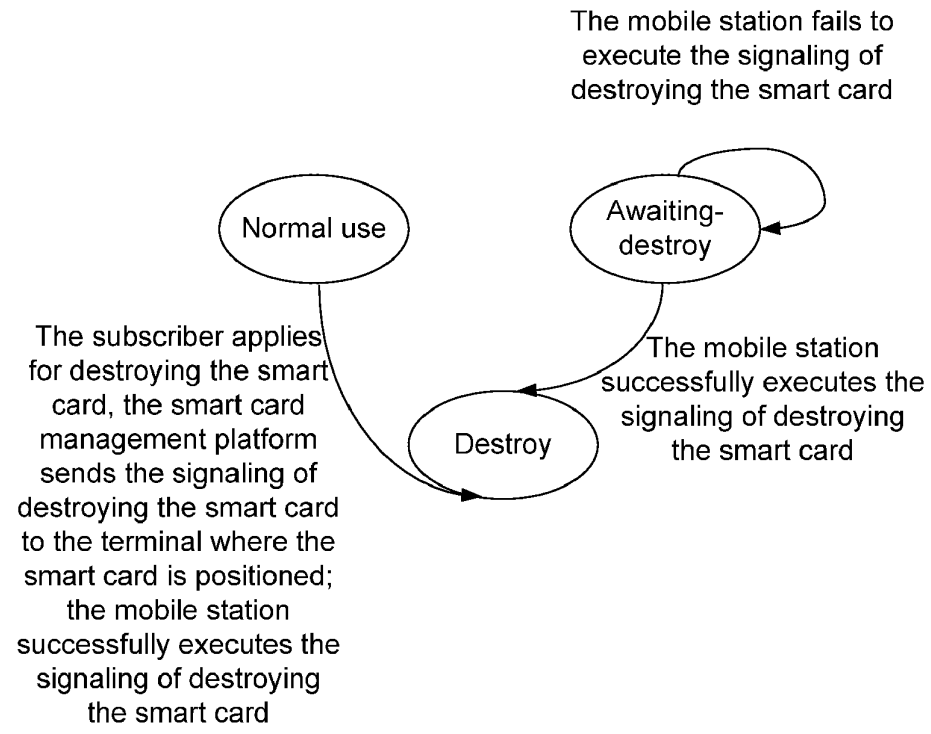

The mobile station fails to execute the signaling of destroying the smart card
Normal use
Awaiting-destroy
The subscriber applies for destroying the smart card, the smart card management platform sends the signaling of destroying the smart card to the terminal where the smart card is positioned; the mobile station successfully executes the signaling of destroying the smart card
The mobile station successfully executes the signaling of destroying the smart card
Destroy

Fig. 6

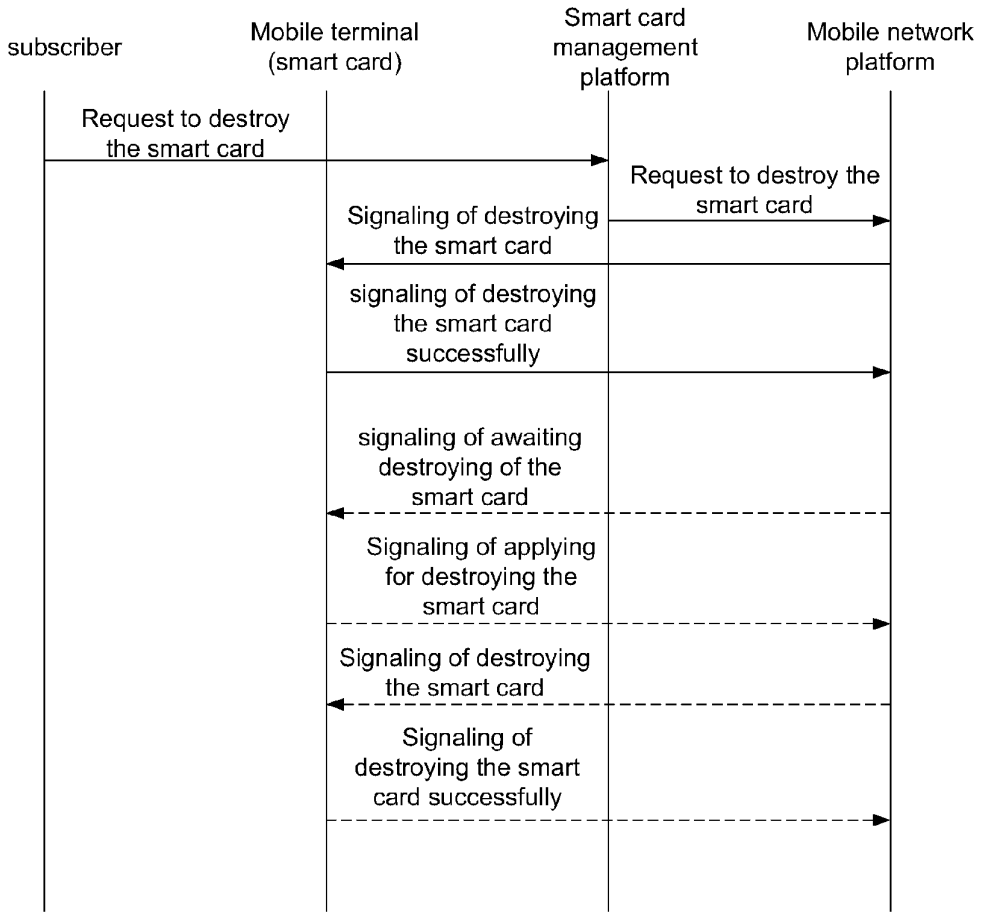

subscriber
Mobile terminal (smart card)
Smart card management platform
Mobile network platform
Request to destroy the smart card
Request to destroy the smart card
Signaling of destroying the smart card
signaling of destroying the smart card successfully
signaling of awaiting destroying of the smart card
Signaling of applying for destroying the smart card
Signaling of destroying the smart card
Signaling of destroying the smart card successfully

Fig. 7

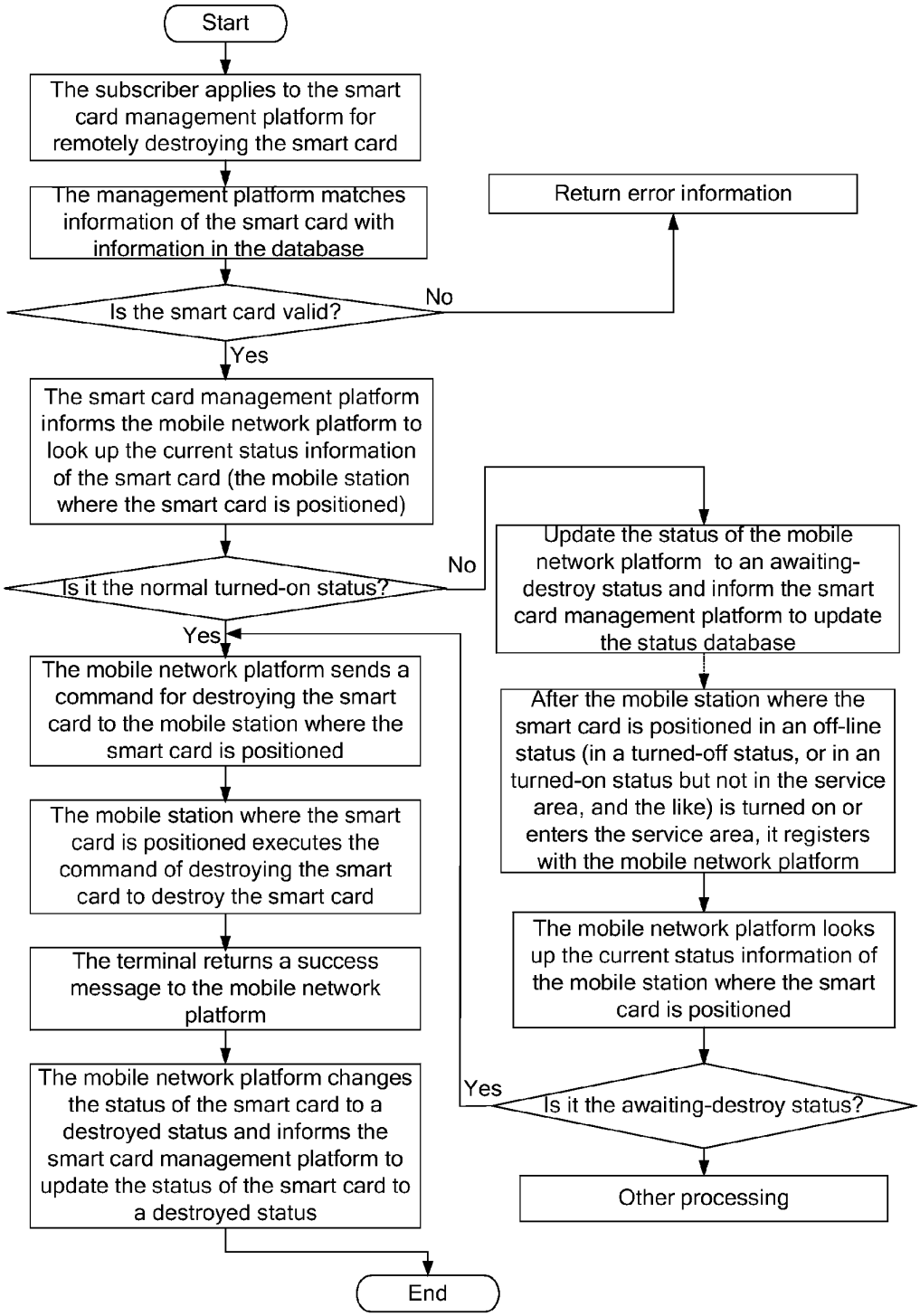

Start
The subscriber applies to the smart card management platform for remotely destroying the smart card
The management platform matches information of the smart card with information in the database
Return error information
Is the smart card valid?
No
Yes
The smart card management platform informs the mobile network platform to look up the current status information of the smart card (the mobile station where the smart card is positioned)
Update the status of the mobile network platform to an awaiting-destroy status and inform the smart card management platform to update the status database
Is it the normal turned-on status?
No
Yes
The mobile network platform sends a command for destroying the smart card to the mobile station where the smart card is positioned
After the mobile station where the smart card is positioned in an off-line status (in a turned-off status, or in an turned-on status but not in the service area, and the like) is turned on or enters the service area, it registers with the mobile network platform
The mobile station where the smart card is positioned executes the command of destroying the smart card to destroy the smart card
The mobile network platform looks up the current status information of the mobile station where the smart card is positioned
The terminal returns a success message to the mobile network platform
Yes
Is it the awaiting-destroy status?
The mobile network platform changes the status of the smart card to a destroyed status and informs the smart card management platform to update the status of the smart card to a destroyed status
Other processing
End

Fig. 8

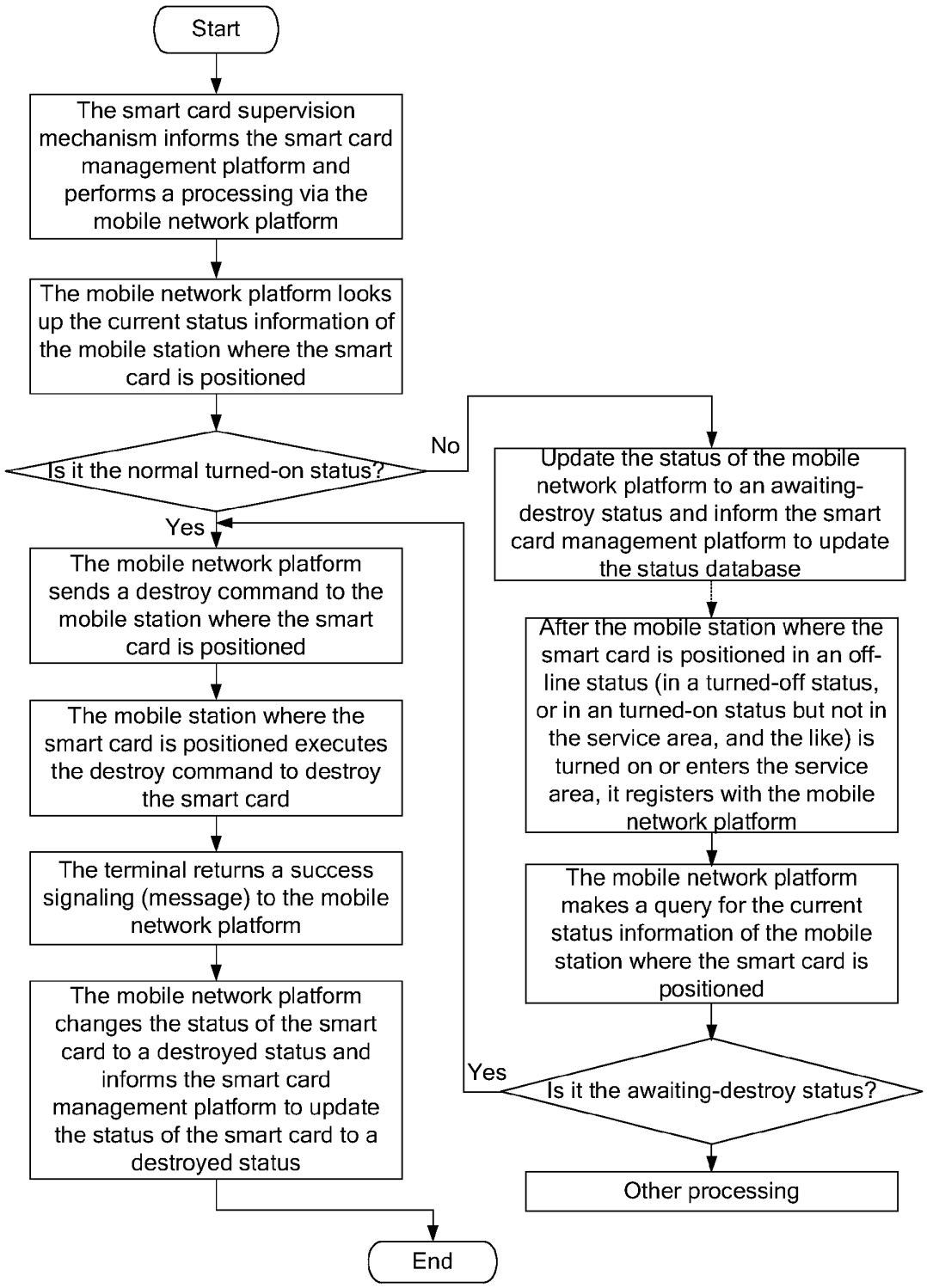

Start
The smart card supervision mechanism informs the smart card management platform and performs a processing via the mobile network platform
The mobile network platform looks up the current status information of the mobile station where the smart card is positioned
Is it the normal turned-on status?
No
Yes
Update the status of the mobile network platform to an awaiting-destroy status and inform the smart card management platform to update the status database
The mobile network platform sends a destroy command to the mobile station where the smart card is positioned
The mobile station where the smart card is positioned executes the destroy command to destroy the smart card
The terminal returns a success signaling (message) to the mobile network platform
The mobile network platform changes the status of the smart card to a destroyed status and informs the smart card management platform to update the status of the smart card to a destroyed status
After the mobile station where the smart card is positioned in an off-line status (in a turned-off status, or in an turned-on status but not in the service area, and the like) is turned on or enters the service area, it registers with the mobile network platform
The mobile network platform makes a query for the current status information of the mobile station where the smart card is positioned
Yes
Is it the awaiting-destroy status?
Other processing
End

Fig. 9

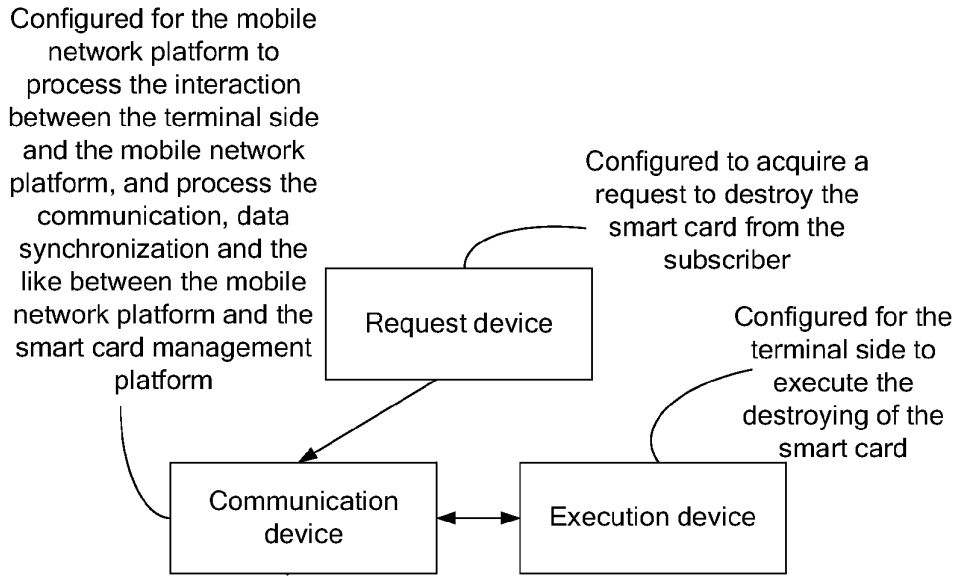

Configured for the mobile network platform to process the interaction between the terminal side and the mobile network platform, and process the communication, data synchronization and the like between the mobile network platform and the smart card management platform
Configured to acquire a request to destroy the smart card from the subscriber
Request device
Configured for the terminal side to execute the destroying of the smart card
Communication device
Execution device

Fig. 10

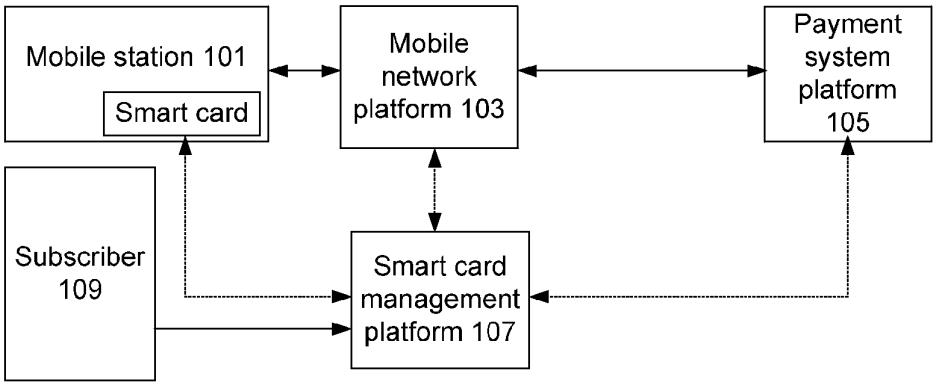

Mobile station 101
Smart card
Mobile network platform 103
Payment system platform 105
Subscriber 109
Smart card management platform 107

Fig. 11

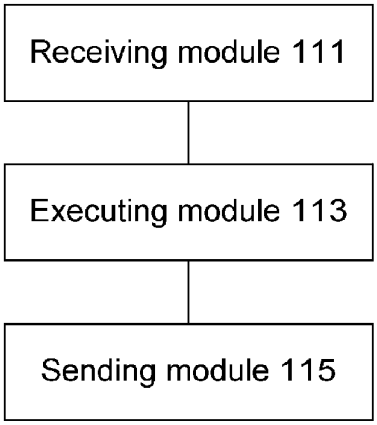
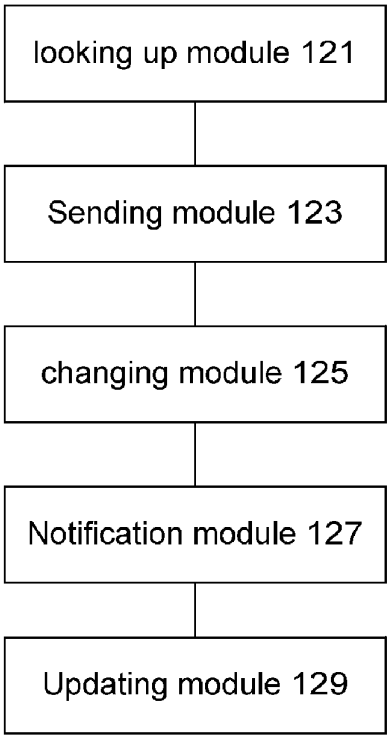

Receiving module 111
Executing module 113
Sending module 115

Fig. 12


looking up module 121
Sending module 123
changing module 125
Notification module 127
Updating module 129

METHOD AND SYSTEM FOR REMOTE CONTROL OF A SMART CARD

TECHNICAL FIELD

[0001] The present application relates to a smart card technology, and in particular to a method and system for remote control of a smart card.

BACKGROUND

[0002] Electronic payment refers to the circulation and payment of funds realized in a computer network system in the form of electronic data storage and transfer by taking commercial electronic tools and various kinds of electronic money as media, and taking computer and communication technology as a means.

[0003] With the combination of Internet, mobile communication and computer and the other technologies in recent years, mobile payment on behalf of mobile electronic commerce emerges as the times require. As an emerging electronic payment manner, the mobile payment is advantaged in that it can be carried out anytime and anywhere, conveniently and fast, and its cost is low, etc. As long as a consumer has a mobile phone, the consumer can complete financing or trading, and enjoy the convenience brought by the mobile payment. Nowadays, the mobile payment is becoming a new highlight in electronic commerce.

[0004] In addition, a recent survey shows that 82% respondents are worried that if their mobile phones are lost or stolen, someone may carry out fraud by making use of the information stored in these mobile phones (including smart cards). Meanwhile, 90% respondents are worried that their personal data and financial data may be lost after their mobile phones are lost; and 72% respondents admit that the information stored in their mobile phones is very important and irreplaceable. Since subscribers use mobile phones to engage in various different activities, such as electronic payment and the like, it is really a disaster for subscribers if their mobile phones are lost. In this survey, **91**% respondents say the loss of mobile phones for electronic payment will bring serious losses to them. Meanwhile, as people increasingly depend on mobile phones, the operator is required to make their own subscribers feel secure. It is good to use mobile phones more widely, however, the mobile operator is required to strengthen the security and management level of personal data information of subscribers in order to nip it in the bud. At present, some solutions have been proposed for the case when mobile phones for electronic payment are lost or stolen. However, these solutions have certain deficiencies, or the processing after a mobile phone for electronic payment is lost or stolen differs greatly from the current payment flow; or due to insufficient security of the system, the payment information of subscribers is still used by others illegally, thus payment is forged; or the system does not deal with the loss of mobile phones timely, which brings huge losses to the subscribers, making the subscribers feel unsecure. At present, no effective solution has been proposed.

SUMMARY

[0005] The present application is proposed based on the problems that: the processing after a mobile phone for electronic payment is lost or stolen differs greatly from the current payment flow; or the system is not secure enough, so payment information of a subscriber is still used by others illegally, resulting in forged payment; or the system does not deal with the loss of a mobile phone timely, which brings huge losses to a subscriber, and makes the subscriber feel unsecure. For this purpose, the present application mainly aims to provide a method and system for remote control of a smart card in order to solve the above problems.

[0006] To achieve the above purpose, according to one aspect of the present application, a method for remote control of a smart card is provided.

[0007] Preferably, a smart card management platform receives a request to destroy a smart card from a subscriber; the smart card management platform performs interactive processing with a terminal side according to the request via a mobile network platform to make the terminal side destroy the smart card.

[0008] Preferably, the terminal side may include a mobile station and a smart card.

[0009] Preferably, the smart card management platform performing interactive processing with the terminal side may include: if the mobile station at the terminal side is in a normal use status, then the mobile station receives a destroy command sent by the mobile network platform; the mobile station destroys the smart card by executing the destroy command.

[0010] Preferably, after the mobile station destroys the smart card, the method may further include: the smart card is in a destroyed status.

[0011] Preferably, after the smart card is in a destroy status, the method may further include: the mobile station returns a destroy success message to the mobile network platform.

[0012] Preferably, the mobile station executing the destroy command to destroy the smart card may include: the mobile station disables function of the smart card by destroying hardware of the smart card; or, the mobile station disables the function of the smart card by executing a preinstalled software procedure.

[0013] Preferably, the method may further include: if the mobile station where the smart card is positioned is in an off-line status, the smart card is updated to an awaiting-destroy status.

[0014] Preferably, after the smart card is updated to an awaiting-destroy status, the method may further include: if the mobile station where the smart card is positioned in an off-line status resumes the normal use status and registers with the mobile network platform, the mobile network platform sends the destroy command to the mobile station where the smart card is positioned; and the mobile station executes the destroy command.

[0015] Preferably, the off-line status may include: the mobile station is in a turned-off status; the mobile station is not in a service area.

[0016] Preferably, after the smart card management platform receives an application from a subscriber, the method may further include: the smart card management platform determines whether the smart card is valid or not.

[0017] Preferably, before the smart card management platform performs interactive processing with the terminal side according to the request via the mobile network platform, the method may further include: the mobile network platform and the terminal side perform security authentication.

[0018] Preferably, after the smart card management platform receives the request to destroy the smart card from the subscriber, the method may further include: the smart card

management platform looks up status information of the mobile station where the smart card is positioned through the mobile network platform.

[0019] Preferably, the smart card management platform looking up status information of the mobile station where the smart card is positioned through the mobile network platform may include: the smart card management platform looks up and finds the status information of the mobile station according to a mobile identification code and location regional information of the mobile station via the mobile network platform.

[0020] Preferably, destroying the smart card may include: if the smart card is in a destroyed status, the smart card cannot be used permanently.

[0021] To achieve the above purpose, according to one aspect of the present application, a method for remote control of a smart card is provided.

[0022] The method for remote control of a smart card according to the present application includes: when a smart card supervision platform finds that a subscriber uses a smart card illegally, the smart card supervision platform informs a smart card management platform to destroy the smart card; the smart card management platform performs interactive signaling processing with a terminal side via a mobile network platform to make the terminal side complete the destroying of the smart card.

[0023] Preferably, the smart card management platform sending a smart card destroy command to the terminal side via the mobile network platform to perform interactive processing may include: the smart card management platform looks up status information of the mobile station where the smart card is positioned via the mobile network platform; if the mobile station is in a normal use status, then the mobile network platform sends a destroy command to the mobile station; the mobile station executes the destroy command to destroy the smart card.

[0024] Preferably, after the mobile station executes the destroy command to destroy the smart card, the method may further include: the mobile station returns a destroy success message to the mobile network platform; the mobile network platform changes a status of the smart card to a destroyed status.

[0025] Preferably, the smart card management platform looking up status information of the mobile station where the smart card is positioned via the mobile network platform may include: the smart card management platform looks up and finds status information of the mobile station according to a mobile identification code and location regional information of the mobile station via the mobile network platform.

[0026] Preferably, after the smart card management platform looking up status information of the mobile station where the smart card is positioned via the mobile network platform, the method may further include: if the mobile station where the smart card is positioned is in an off-line status, then the mobile network platform updates its status to an awaiting-destroy status.

[0027] To achieve the above purpose, according to another aspect of the present application, a system for remote control of a smart card is provided.

[0028] The system for remote control of a smart card according to the present application includes: a mobile network platform configured to send a destroy command; and a mobile station configured to execute the destroy command to destroy a smart card.

[0029] Preferably, the system may further include: a smart card management platform configured to receive a request from a subscriber and perform signaling interaction with the mobile station via the mobile network platform.

[0030] Preferably, the smart card management platform may be further configured to monitor whether the subscriber uses the smart card illegally.

[0031] Preferably, the mobile network platform may be further configured to look up status information of the mobile station where the smart card is positioned.

[0032] To achieve the above purpose, according to another aspect of the present application, a mobile terminal is provided.

[0033] The mobile terminal according to the present application includes: a receiving module configured to receive a request to destroy a smart card; and an executing module configured to execute destroying of the smart card.

[0034] Preferably, the mobile terminal may further include: a sending module, configured to send a destroy success message.

[0035] To achieve the above purpose, according to another aspect of the present application, a mobile network platform is provided.

[0036] The mobile network platform according to the present application includes: a sending module configured to send a destroy command to a mobile station when the mobile station is in a normal use status; an changing module, configured to chang a status of a smart card; an updating module, configured to update a status of the smart card, update the status of the smart card to a destroyed status when the mobile station and the smart card are in an on-line status and the destroy process is successfully executed, and update the status of the smart card to an awaiting-destroy status when the mobile station and the smart card are in an off-line status.

[0037] Preferably, the mobile network platform may further include: a notification module, configured to inform the smart card management platform to update a status of the smart card to a destroyed status.

[0038] Through the present application, the smart card management platform receives a request to destroy the smart card from a subscriber; according to the request, the smart card management platform performs interactive processing with the terminal side via the mobile network platform to make the terminal side destroy the smart card, therefore solving the problems that: the processing after the mobile phone for electronic payment is lost or stolen differs greatly from the current payment flow; or the system is not secure enough, thus payment information of a subscriber is still used by others illegally, resulting in forged payment; or the system does not deal with the loss of the mobile phone timely, which brings huge losses to a subscriber and makes the subscriber feel unsecure, therefore further avoiding the loss caused when a subscriber terminal for payment is robbed, lost, stolen, or is used illegally seriously, and providing a higher flexibility to the payment system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0039] FIG. **1** shows a flowchart of a method for remote control of a smart card according to an embodiment of the present application;

[0040] FIG. **2** shows a preferred flowchart of the method for remote control of a smart card according to an embodiment of the present application;

[0041] FIG. **3** shows a preferred flowchart of the method for remote control of a smart card according to an embodiment of the present application;

[0042] FIG. **4** shows a schematic diagram of a status machine at a network side according to an embodiment of the present application;

[0043] FIG. **5** shows a schematic diagram of a status machine at a terminal side according to an embodiment of the present application;

[0044] FIG. **6** shows a schematic diagram of signaling interaction in a system according to an embodiment of the present application;

[0045] FIG. **7** shows a preferred flowchart of the method for remote control of a smart card according to an embodiment of the present application;

[0046] FIG. **8** shows a preferred flowchart of the method for remote control of a smart card according to an embodiment of the present application;

[0047] FIG. **9** shows a schematic diagram of a preferred system for remote control of a smart card according to an embodiment of the present application;

[0048] FIG. **10** shows a schematic diagram of a preferred system for remote control of a smart card according to an embodiment of the present application;

[0049] FIG. **11** shows a schematic diagram of a mobile station according to an embodiment of the present application; and

[0050] FIG. **12** shows a schematic diagram of a mobile network platform according to an embodiment of the present application.

DETAILED DESCRIPTION

[0051] Considering the problems that: the processing after a mobile phone for electronic payment is lost or stolen differs greatly from the current payment flow; or the system is not secure enough, therefore the payment information of a subscriber is still used by others illegally, which results in forged payment; or the system does not deal with the loss of a mobile phone timely, which brings huge losses to a subscriber and make the subscriber feel unsecure; embodiments of the present application provides a method and system for remote control of a smart card. The method comprises: a smart card management platform receives a request to destroy a smart card from a subscriber; according to the request, the smart card management platform performs interactive processing with a terminal side via a mobile network platform to make the terminal side destroy the smart card.

[0052] It should be noted that, if no conflict is caused, the embodiments in the application and the features in the embodiments can be combined with each other. The present application is described below with reference to the accompanying drawings and embodiments in detail.

[0053] According to an embodiment of the present application, a method for remote control of a smart card is provided.

[0054] FIG. **1** shows a flowchart of the method for remote control of a smart card according to the embodiment of the present application.

[0055] As shown in FIG. **1**, the method comprises the following step S**101** to step S**103**:

[0056] step S**101**: a smart card management platform receives a request to destroy a smart card from a subscriber; and

[0057] step S**103**: according to the request, the smart card management platform performs interactive processing with a terminal side via a mobile network platform to make the terminal side destroy the smart card.

[0058] The implementation process of this embodiment of the present application is described below with reference to examples in detail.

[0059] FIG. **3** shows a preferred flowchart of the method for remote control of a smart card according to the embodiment of the present application; as shown in FIG. **3**, the method for remote control of a smart card comprises:

[0060] S**11**, if a smart card supervision mechanism (such as a payment system platform or the smart card management platform) finds that a subscriber uses a smart card illegally, the smart card supervision mechanism informs the mobile network platform to process this case;

[0061] S**12**, the smart card management platform performs short message interaction with the terminal side where the smart card is positioned via the mobile network platform to execute the destroying of the smart card; and

[0062] S**13**, the terminal completes the destroying of the smart card.

[0063] According to one aspect of the present application, a method for destroying a smart card remotely based on electronic payment service is provided.

[0064] FIG. **2** shows a preferred flowchart of the method for remote control of a smart card according to the embodiment of the present application. FIG. **4** shows a schematic diagram of a status machine at a network side according to the embodiment of the present application. FIG. **5** shows a schematic diagram of a status machine at a terminal side according to the embodiment of the present application.

[0065] As shown in FIG. **2**, with reference to FIG. **4** and FIG. **5**, the method for remote control of a smart card comprises:

[0066] step S**1**, the subscriber applies to the smart card management platform for destroying the smart card;

[0067] step S**2**, the mobile network platform and the terminal side (the terminal, the smart card) perform interactive signaling processing; and

[0068] step S**3**, the terminal side completes destroying the smart card.

[0069] FIG. **7** shows a preferred flowchart of the method for remote control of a smart card according to the embodiment of the present application; with reference to FIG. **7**, the step S**2** may comprise the following processes:

[0070] step S**100**, after receiving the request to destroy the smart card sent from the subscriber to the smart card management platform, the management platform matches information of the smart card with information in the database to determine if the smart card is valid; if the smart card is invalid, then the management platform returns a failure message and the current processing flow is ended; and if the smart card is valid, then the next step is executed;

[0071] step S**102**, the smart card management platform looks up current status information of a mobile station where the smart card is positioned via the mobile network platform; if the mobile station where the smart card is positioned is in a normal turned-on status, then the mobile network platform directly sends a destroy command to the mobile station where the smart card is positioned, and, after the mobile station where the smart card is positioned executes the destroy command to destroy the smart card, the mobile station returns a success message to the mobile network platform, and the

mobile network platform changes the status of the smart card to a destroyed status and informs the smart card management platform to update the status of the smart card to a destroyed status; if the mobile station where the smart card is positioned is in an off-line status (in a turned-off status, or in an turned-on status but not in a service area, and the like), then the mobile network platform updates its status to an awaiting-destroy status, and informs the smart card management platform to update a status database; and

[0072] step S**104**, after the mobile station where the smart card is positioned in an off-line status (in a turned-off status, or in an turned-on status but not in a service area, and the like) is turned on or enters the service area, when it registers with the mobile network platform, the mobile network platform makes a query and finds that the mobile station where the smart card is positioned is in an awaiting-destroy status, and sends a destroy command to the mobile station where the smart card is positioned; after executing the destroy command to destroy the smart card, the mobile station returns a success message to the mobile network platform, and the mobile network platform updates theist status to a destroyed status and informs the smart card management platform to synchronously update the status database.

[0073] In the method, before the mobile station where the smart card is positioned executes the destroy command sent by the mobile network platform in step S**102**/S**104**, a security authentication should be included in order to confirm the command is the destroy command sent by the smart card management platform.

[0074] FIG. **6** shows a schematic diagram of signaling interaction in a system according to an embodiment of the present application; as shown in FIG. **6**, signaling interaction between a subscriber and the mobile network platform is realized through signaling as shown.

[0075] In the method, the step S**102** that the mobile station where the smart card is positioned executes the destroy command to destroy the smart card comprises:

[0076] step S**201**, the mobile station disables the function of the smart card permanently by destroying physical (or the smart card) hardware; and

[0077] step S**202**, the mobile station destroys the smart card by executing a preinstalled software procedure (device).

[0078] In the step S**202**, the preinstalled software procedure (device) can either be preinstalled in the smart card, or be preinstalled in the mobile station where the smart card is positioned.

[0079] For example, in a method for destroying a smart card by destroying hardware, the voltage of a mobile phone battery is directly applied to the power supply circuit of the smart card; since the normal voltage of the smart card is quite lower (1.8 v/3 v), while the operating voltage of a mobile terminal is generally 3.6 v to 4.2 v (other destroy methods can be employed for a card under 5 v), the smart card can be destroyed directly, and cannot be repaired.

[0080] The software procedure is preinstalled in the terminal where the smart card is positioned, and the step that the mobile station executes the destroy command is as follows:

[0081] step S**300**, destroying payment data in the smart card (the memory where the payment data is stored); and

[0082] step S**302**, executing the preinstalled software procedure in the terminal to destroy a payment data smart card program in the smart card;

[0083] the software procedure is preinstalled in the smart card, and the step that the mobile station executes a command to destroy the payment data in the smart card is as follows:

[0084] step S**3020**, copying the preinstalled software procedure in the smart card into the terminal;

[0085] step S**3021**, destroying the payment data in the smart card (the memory where the payment data is stored); and

[0086] step S**3022**, executing the copied software procedure in the terminal, which is a back-up program of destroying the smart card.

[0087] For example, if the smart card is to be destroyed by a software program, the software program may be written to make the number of times of inputting PUK codes greater than 10, then the smart card is permanently locked and cannot be unlocked, namely the smart card is destroyed.

[0088] In step S**102** that the smart card management platform looks up the current status information of the mobile station where the smart card is positioned via the mobile network platform, the mobile network platform finds the status information of the mobile station according to the mobile identification code and the location regional information of the mobile station.

[0089] Step S**104**, after the mobile station where the smart card is positioned in an off-line status (in a turned-off status, or in an turned-on status but not in a service area, and the like) is turned on or enters the service area, when it registers with the mobile network platform, the mobile network platform makes a query and finds that the mobile station where the smart card is positioned is in an awaiting-destroy status, and sends a destroy command to the mobile station where the smart card is positioned; after executing the destroy command to destroy the smart card, the mobile station returns a success message to the mobile network platform, and the mobile network platform updates its status to a destroyed status and informs the smart card management platform to synchronously update the status database.

[0090] According to another aspect of the present application, a method for destroying a smart card remotely based on an electronic payment service is provided (in this method, a subscriber does not need to apply, but the management platform directly handles the destroying of a smart card of the subscriber, which is corresponding to the case that the smart card is used illegally by the subscriber).

[0091] FIG. **3** shows a preferred flowchart of the method for remote control of a smart card according to an embodiment of the present application; FIG. **8** shows a preferred flowchart of the method for remote control of a smart card according to an embodiment of the present application.

[0092] As shown in FIG. **3**, with reference to FIG. **8**, the method for remote control of a smart card comprises:

[0093] S**11**, if the smart card supervision mechanism (such as the payment system platform or the smart card management platform) finds that a subscriber uses the smart card illegally, the smart card supervision mechanism informs the mobile network platform to process this case;

[0094] S**12**, the smart card management platform performs short message interaction with the terminal side where the smart card is positioned via the mobile network platform to execute the destroying of the smart card; and

[0095] S**13**, the terminal completes the destroying of the smart card.

[0096] Wherein step S**12** may comprise the following processes:

[0097] step S**402**, the smart card management platform looks up the current status information of the mobile station where the smart card is positioned via the mobile network platform; if the mobile station where the smart card is positioned is in a normal turned-on status, the mobile network platform sends a destroy command to the mobile station where the smart card is positioned directly; after the mobile station where the smart card is positioned executes the destroy command to destroy the smart card, the mobile station returns a success message to the mobile network platform; the mobile network platform changes the status of the smart card to a destroyed status and informs the smart card management platform to update the status of the smart card to a destroyed status; if the mobile station where the smart card is positioned is in an off-line status (in a turned-off status, or in an turned-on status but not in a service area, and the like), the mobile network platform updates its status to an awaiting-destroy status, and informs the smart card management platform to update the status database;

[0098] step S**404**, after the mobile station where the smart card is positioned in an off-line status (in a turned-off status, or in an turned-on status but not in a service area, and the like) is turned on or enters the service area, when it registers with the mobile network platform, the mobile network platform makes a query and finds that the mobile station where the smart card is positioned is in an awaiting-destroy status, and sends a destroy command to the mobile station where the smart card is positioned; after executing the destroy command to destroy the smart card, the mobile station returns a success message to the mobile network platform; the mobile network platform updates its status to a destroyed status and informs the smart card management platform to synchronously update the status database.

[0099] In the method, before the mobile station where the smart card is positioned executes the destroy command sent by the mobile network platform in step S**402**/S**404**, a security authentication should be included in order to confirm the command is the destroy command sent by the smart card management platform.

[0100] In the method, the step S**402** that the mobile station where the smart card is positioned executes the destroy command to destroy the smart card comprises:

[0101] step S**501**, the mobile station disables the function of the smart card permanently by destroying physical hardware; and

[0102] step S**502**, the mobile station destroys the smart card by executing a preinstalled software procedure (device).

[0103] In the step S**502**, the preinstalled software procedure (device) can either be preinstalled in the smart card, or be preinstalled in the mobile station where the smart card is positioned.

[0104] For example, if the smart card is to be destroyed by destroying hardware, the voltage of the mobile phone battery may be directly applied to the power supply circuit of the smart card; since the normal voltage of the smart card is quite lower (1.8 v/3 v), while the operating voltage of the mobile terminal is generally 3.6 v to 4.2 v (other destroy methods can be employed for the card under 5 v), the smart card can be destroyed directly, and cannot be repaired.

[0105] The software procedure is preinstalled in the terminal where the smart card is positioned, and the step that the mobile station executes the destroy command is as follows:

[0106] step S**600**, destroying payment data in the smart card (the memory where the payment data is stored);

[0107] step S**602**, executing the preinstalled software procedure in the terminal to destroy a payment data smart card program in the smart card;

[0108] the software procedure is preinstalled in the smart card, and the step that the mobile station executes a command to destroy the payment data in the smart card is as follows:

[0109] step S**602**, copying the preinstalled software procedure in the smart card into the terminal;

[0110] step S**604**, destroying the payment data in the smart card (the memory where the payment data is stored);

[0111] step S**606**, executing the copied software procedure in the terminal, which is a back-up program of destroying the smart card.

[0112] For example, if the smart card is to be destroyed by a software program, the software program may be written to make the number of times of inputting PUK codes greater than 10, then the smart card is permanently locked and cannot be unlocked, namely the smart card is destroyed.

[0113] In addition, step S**402**, the smart card management platform looks up the current status information of the mobile station where the smart card is positioned via the mobile network platform, and the mobile network platform finds the status information of the mobile station according to the mobile identification code and the location regional information of the mobile station.

[0114] Step S**404**, after the mobile station where the smart card is positioned in an off-line status (in a turned-off status, or in an turned-on status but not in a service area, and the like) is turned on or enters the service area, when it registers with the mobile network platform, the mobile network platform makes a query and finds that the mobile station where the smart card is positioned is in an awaiting-destroy status, and sends a destroy command to the mobile station where the smart card is positioned; after executing the destroy command to destroy the smart card, the mobile station returns a success message to the mobile network platform; the mobile network platform updates its status to a destroyed status and informs the smart card management platform to update synchronously the status database.

[0115] According to another aspect of the present application, a device for destroying a smart card remotely based on an electronic payment service is provided, comprising:

[0116] a smart card management platform, which includes but is not limited to a smart card application management system for providing and managing applications owned by or entrusted to a smart card issuer; which further includes a smart card application provider management platform, through the system, relevant information of the smart card application provider is recorded, and service authorities of the smart card application provider and the like are specified;

[0117] a request device, which is configured to acquire a request from a subscriber;

[0118] a communication device, which is configured for a mobile network platform to process interaction between a mobile station and the mobile network platform, and process communication, data synchronization and the like between the mobile network platform and the card management platform;

[0119] an execution device, which is configured for a mobile station to execute destroying of a smart card.

[0120] The smart card includes, but is not limited to an sim card, an R-UIM card, a usim card, a csim card, a UICC card,

a java card, a financial card, a traffic card, a prepaid card and combined cards of the above cards.

[0121] The mobile terminal or mobile station includes, but is not limited to a terminal such applying to GSM, CDMA, WCDMA, Td-Scdma, cdma2000, data card, fixed station, LTE, LTE+ and the like, and a multi-mode terminal of any combination thereof.

Device Embodiment

[0122] According to an embodiment of the present application, a system for remote control of a smart card is provided.

[0123] FIG. **9** shows a schematic diagram of a preferred system for remote control of a smart card according to an embodiment of the present application.

[0124] As shown in FIG. **9**, the system comprises a request device, a communication device and an execution device.

[0125] Specifically, the request device is configured to acquire a request from a subscriber;

[0126] the communication device is configured for a mobile network platform to process interaction between a mobile station and the mobile network platform, for implementing communication, data synchronization and the like between the mobile network platform and the card management platform; the execution device is configured for the mobile station to destroy a smart card.

[0127] FIG. **10** shows a schematic diagram of a preferred system for remote control of a smart card according to an embodiment of the present application.

[0128] As shown in FIG. **10**, the system comprises a mobile network platform **103**, a mobile station **101**, a smart card management platform **107**, a payment system platform **105**, wherein both the mobile network platform **103** and the smart card management platform **107** are connected to the payment system platform **105**.

[0129] The mobile network platform **103** is configured to send a destroy command to the mobile station; and the mobile station **101** is configured to execute the destroy command to destroy the smart card.

[0130] Preferably, when a subscriber **109** applies to the smart card management platform **107** for destroying a smart card, the smart card management platform **107** looks up the current status information of the mobile station where the smart card is positioned via the mobile network platform; if the mobile station where the smart card is positioned is in a normal turned-on status, the mobile network platform **103** directly sends a destroy command to the mobile station **101** where the smart card is positioned; after the mobile station **101** where the smart card is positioned executes the destroy command to destroy the smart card, the mobile station **101** where the smart card is positioned returns a success message to the mobile network platform **103**; the mobile network platform **103** changes the status of the smart card to a destroyed status and informs the smart card management platform **107** to update the status of the smart card to a destroyed status; if the mobile station **101** where the smart card is positioned is in an off-line status (in a turned-off status, or in an turned-on status but not in a service area, and the like), the mobile network platform **103** updates the status of the smart card to an awaiting-destroy status, and informs the smart card management platform **107** to update the status database.

[0131] FIG. **11** shows a schematic diagram of a mobile station according to an embodiment of the present application.

[0132] As shown in FIG. **11**, the mobile terminal comprises: a receiving module **111**, an executing module **113** and a sending module **115**.

[0133] Specifically, the receiving module **111** is configured to receive a request to destroy a smart card; the executing module **113** is configured to execute the destroying of the smart card; the sending module **115** is configured to send a destroy success message.

[0134] FIG. **12** shows a schematic diagram of a mobile network platform according to an embodiment of the present application.

[0135] As shown in FIG. **12**, the mobile network platform comprises: a looking up module **121**, a sending module **123**, a changing module **125** and an updating module **129**, and may further comprise a notification module **127**.

[0136] Specifically, the looking up module **121** is configured to look up the status information of the mobile station where the smart card is positioned; the sending module **123** is configured to, when the status information of the mobile station indicates that the mobile station is in a normal use status, send a destroy command to the mobile station; the changing module **125** is configured to change the status of the smart card to a destroyed status; the notification module **127** is configured to inform the smart card management platform to update the status of the smart card to a destroyed status; the updating module **129** is configured to, when the status information indicates that the mobile station where the smart card is positioned is in an off-line status, update its status to an awaiting-destroy status.

[0137] It can be seen from the above description that the present application can avoid the loss caused when a subscriber terminal for payment is robbed, lost, stolen, or is used illegally seriously, and provides a higher flexibility to the payment system.

[0138] The above are only preferred embodiments of the present application and not intended to limit the present application, and those skilled in the art can make various alternations and changes to the present application. Any modifications, equivalent replacements, improvements and the like within the spirit and principle of the present application shall fall within the scope of protection of the present application.

1. A method for remote control of a smart card which is included in a terminal side, comprising:

receiving, by a smart card management platform, a request to destroy the smart card from a subscriber;

performing, by the smart card management platform, signaling interaction with the terminal side via a mobile network platform to control the terminal side to destroy the smart card.

2. The method according to claim **1**, wherein the terminal side further comprises a mobile station, and the smart card management platform performing signaling interaction with the terminal side comprises:

when the mobile station is in a normal use status, the mobile station receives a destroy command from the mobile network platform;

the mobile station executes the destroy command to destroy the smart card.

3. The method according to claim **2**, further comprising: after the mobile station destroys the smart card, the smart card being in a destroyed status;

wherein after the smart card is in the destroyed status, the mobile station returns a destroy success message to the mobile network platform.

4. (canceled)

5. The method according to claim **2**, wherein the mobile station executing the destroy command to destroy the smart card comprises:

the mobile station disables function of the smart card by destroying hardware of the smart card; or

the mobile station disables the function of the smart card by executing a preinstalled software procedure.

6. The method according to claim **2**, further comprising:

updating the smart card to an awaiting-destroy status when the mobile station where the smart card is positioned is in an off-line status;

sending the destroy command by the mobile network platform to the mobile station where the smart card is positioned when the mobile station where the smart card is positioned registers with the mobile network platform, and executing the destroy command by the mobile station.

7. The method according to claim **6**, wherein the off-line status comprises:

the mobile station is in a turned-off status;

or the mobile station is not in a service area.

8. The method according to claim **1**, further comprising: after the smart card management platform receives an application from a subscriber, determining, by the smart card management platform, whether the smart card is valid or not.

9. The method according to claim **1**, further comprising: before the smart card management platform performs signaling interaction with the terminal side via the mobile network platform, performing security authentication between the mobile network platform and the terminal side.

10. The method according to claim **1**, further comprising: after the smart card management platform receives a request to destroy the smart card from the subscriber, the smart card management platform looking up off-line or on-line status information of the mobile station where the smart card is positioned through the mobile network platform.

11. The method according to claim **10**, wherein the smart card management platform looking up off-line or on-line status information of the mobile station where the smart card is positioned through the mobile network platform comprises:

the smart card management platform looks up and finds the off-line or on-line status information of the mobile station according to a mobile identification code and location regional information of the mobile station via the mobile network platform.

12. A method for remote control of a smart card, comprising:

informing, by a smart card supervision platform, a smart card management platform to destroy the smart card when the smart card supervision platform finds that a subscriber uses the smart card illegally;

performing, by the smart card management platform, signaling interaction with a terminal side via a mobile network platform to control the terminal side to complete the destroying of the smart card.

13. The method according to claim **12**, wherein the smart card management platform sending a command to destroy the smart card to the terminal side via the mobile network platform comprises:

the smart card management platform looks up status information of a mobile station where the smart card is positioned via the mobile network platform;

when the mobile station is in a normal use status, the mobile network platform sends a destroy command to the mobile station;

the mobile station executes the destroy command to destroy the smart card.

14. The method according to claim **13**, further comprising: after the mobile station executes the destroy command to destroy the smart card,

returning a destroy success message by the mobile station to the mobile network platform;

changing a status of the smart card to a destroyed status by the mobile network platform.

15. The method according to claim **14**, wherein the smart card management platform looking up status information of the mobile station where the smart card is positioned via the mobile network platform comprises:

the smart card management platform looks up and finds the status information of the mobile station according to a mobile identification code and location regional information of the mobile station via the mobile network platform.

16. The method according to claim **14**, further comprising: after the smart card management platform looks up the status information of the mobile station where the smart card is positioned via the mobile network platform,

updating, by the mobile network platform, a status of the mobile network platform to an awaiting-destroy status when the mobile station where the smart card is positioned is in an off-line status.

17. A system for remote control of a smart card, comprising:

a mobile network platform configured to send a destroy command;

a mobile station configured to execute the destroy command to destroy the smart card.

18. The system according to claim **17**, further comprising:

a smart card management platform, configured to receive a request from a subscriber and perform signaling interaction with the mobile station via the mobile network platform.

19. The system according to claim **18**, wherein the mobile network platform is further configured to look up status information of the mobile station where the smart card is positioned.

20. A mobile terminal, comprising a mobile station and a smart card, and further comprising:

a receiving module, configured to receive a request to destroy the smart card;

an executing module, configured to execute destroying of the smart card; and

a sending module, configured to send a destroy success message.

21. (canceled)

22. A mobile network platform, comprising:

a sending module, configured to send a destroy command to a mobile station when the mobile station is in a normal use status; and

an updating module, configured to update a status of a smart card; updating the status of the smart card to a destroyed status when the mobile station and the smart card are in an on-line status and the destroy command is successfully executed; and updating the status of the smart card to an awaiting-destroy status when the mobile station and the smart card are in an off-line status.

* * * * *