A METHOD AND SYSTEM FOR SECURELY AND AUTOMATICALLY DOWNLOADING A MASTER KEY IN A BANK CARD PAYMENT SYSTEM

Technical Field

The present invention relates to a bank card payment system, and more particularly, to a secure method for protecting a master key in the bank card payment system.

Background

The bank card, as a payment tool, is becoming more and more popular. A typical bank card payment system includes a Point Of Sale (POS), a Terminal Management System (TMS), a PIN PAD, and a Hardware and Security Module (HSM).

The POS terminal is a device that is able to receive bank card information, has communication capability, and is able to receive a clerk's instructions to complete the exchange of financial transaction information and other related information. The TMS system is a centralized management and transaction processing system that makes centralized management of its POS terminals, including downloading parameters, downloading keys, receiving, processing, or forwarding transaction requests from the POS Terminals, and sending the results information of the transaction back to the POS terminals. The PIN PAD is a secure device for securely storing and protecting TMK, PIK and MAK, and encrypting PINs. The HSM is a peripheral device for encrypting the transmitted data, and is used for encrypting/decrypting, verifying the reliability of messages and documents, and storing keys. The Personal Identification Number (PIN), i. e., the personal password, is data information for identifying the validity of a card holder’s identity in the online transaction, and is never allowed to be exposed in plaintext at any stage of the computer and network system. The TMK (Terminal Master Key) is a mater key that encrypts a working key (WK) when the POS terminal is working, and it is stored in the system hardware. The TMK is readable but not writable. The working key (WK), also referred to as a data key, typically includes a PIN encrypting key (PIK) and a message authentication

code (MAC) key (MAK). The working key is required to be updated frequently. The working key is required to be encrypted in the message updated online by the TMK to generate a cipher text prior to transmission.

The POS terminals are widely used in bank card payment scenarios, such as mall shopping, and hotel authentication, etc., and they are indispensable modern payment means which has come into our daily life. Bank cards, especially debit cards, are usually set up with a PIN by the card's holder. During the payment, in addition to uploading information such as the magnetic track information of the bank card, the POS terminals also require the card's holder to enter the PIN so as to enable the bank which issued the card to authenticate the validity of the card holder's identity to ensure the security of the bank card payment and to protect the financial security of the card's holder. In order to prevent the PINs from being exposed or cracked, it is required that the PINs need to stay encrypted during the entire information exchange process from the terminals to the bank. The PINs are not allowed to expose in plaintext at any stage of the computer and network system. To that end, all POS terminals that can accept PINs are required to be provided with a key management system.

The key systems for POS terminals are divided into two levels: the Terminal Master Key (TMK) and the working key (WK). Wherein the TMKs protect the WKs during the updating of the WKs by encrypting them. Each POS terminal and TMS share a unique TMK. There needs to be a security mechanism to ensure that the TMK can only be written into the hardware device and involved in computing process, but can not be read. The WK includes a PIK, which is used for encrypting the PIN, and a message authentication code (MAC) key (MAK), both of which are generated by a TMS invoking an HSM, and they are downloaded when the POS terminal check in at the TMS, and are encrypted by utilizing the TMK during transmission and storage, wherein the encryption algorithm is the 3DES algorithm which has a high security level. The detailed procedure of downloading a working key is shown in Fig. 1:

The POS terminal sends a check-in request to the TMS;

The TMS invokes the HSM to randomly generate the PIK and the MAK encrypted with the TMK;

The POS terminal receives the PIK and MAK cipher texts from the TMS and stores

them into the PIN PAD.

During the bank card payment procedure, the PIN, after being entered through the PIN PAD by the card holder, is encrypted with the PIK by the PIN PAD and then uploaded to the TMS. Next, the encrypted PIN is translated by the TMS invoking the HSM, and then it is sent to the bank which issued the card for authentication. During the entire transmission process, it is ensured that the PIN is encrypted and protected by hardware, and the 3DES encryption algorithm used is one of the encryption algorithms that are widely used and have high security level, which is typically used in the financial industry.

As can be seen from above procedure of downloading the working key, the TMK is a crucial root key. If the TMK was intercepted, the PIK, MAK, or even PIN could be cracked by using the 3DES algorithm, which is a great threat to the security of bank card payment. Therefore, it is a crucial for key security whether or not the TMK can be securely downloaded to the POS terminals. Several existing methods for downloading the TMK are listed as bellow:

The TMK plaintext is generated by the TMS, and is directly entered into the PIN PAD of a POS terminal manually. There are severe security flaws in this method in that the TMK plaintext can be readily accessed by a specific operator, and there also exists the possibility that it is incorrectly entered manually, and thus this significantly affect the subsequent downloading of the working key and the encryption of the PIN.

Plaintext is imported from the IC card, the TMK plaintext is generated by the TMS, then is written into the IC card, and eventually the POS terminal read the TMK plaintext from the IC card and store it in the PIN PAD. There also exist several severe security flaws in this method in that the TMK plaintext is stored in the IC card. The TMK plaintext can be easily accessed as long as an IC card reader is available, and thus this significantly affect the subsequent downloading of the working key and the encryption of the PIN.

The TMK cipher text is imported from the IC card, the TMK generated by the TMS is encrypted with a specified key (known as transmission key for short) before being stored into the IC card. The POS terminal read the TMK cipher text from the IC card and then decrypt it with an IC card storing the transmission key, and eventually import it into the PIN PAD. This method is an improvement, since an encrypted transmission is incorporated

while the IC card is still entered in plaintext manner. Only the person who has the IC card with the transmission key stored therein is able to obtain the TMK plaintext, and thus the insecurity during the transmission of the key is reduced.

The TMK cipher text is imported from a special POS terminal, called parent POS terminal, the TMK cipher text generated by the TMS is decrypted by the parent POS terminal and then is imported directly into a POS terminal connected to the parent POS terminal via a serial connection, thereby the insecurity during the importing of the key is reduced. This method has a security level that is the same as that of the method in which the TMK cipher text is imported from the IC card, but there exists the following disadvantages: it is inconvenient to carry the terminals, and it is difficult to import the TMK at the site of the merchants.

In summary, the main defects of the existing methods for downloading the TMK are as follows:

There exists possibility of manmade mistakes in the method in which data is entered manually.

Inputting the TMK in plaintext manner may cause severe security flaws and the plaintext is easy to be intercepted, especially by the person who manually enters the data.

IC cipher text importing and parent POS importing partly overcome the potential insecurity during the transmission, but there still exists insecurities in the maintenance and carrying of the transmission key IC card and the parent POS.

All the aforementioned methods for downloading the TMK need human intervention to directly operate the POS terminal, that is, they require technical support personnel to arrive at the site where the POS is located to complete the downloading task, and therefore the cost of labor is high, especially when there are a great number of POS terminals and the terminals are severely malfunctioning.

Summary

The object of the present invention is to provide a method for securely and automatically downloading a master key so as to eliminate the security flaws in the downloading process of the master key.

A method for securely and automatically downloading a master key TMK in a bank card payment system is disclosed, wherein the bank card payment system includes a Point Of Sale POS, a Terminal Management system TMS, a PIN PAD, and a HSM. A pair of public and private keys are generated by the TMS invoking the HSM. The master key TMK is generated randomly by the POS terminal invoking the PIN PAD. The TMK is encrypted with the public key of the TMS, and then is uploaded to the TMS. The TMK is decrypted with the private key by the TMS invoking the HSM. The decrypted TMK is stored by the TMS.

Additionally, a pair of public and private keys are generated by the TMS invoking the HSM, wherein the private key is stored in the HSM and the public key is stored in a database of the TMS. The POS terminals initiate a request for downloading the public key, and receive the public key returned by the TMS, and then store the public key into the PIN PAD.

Additionally, the TMS decrypts the encrypted TMK with the private key by invoking the HSM after the encrypted TMK is received from the POS terminal; and directly stores the TMK plaintext into the HSM. If the HSM does not have the storage capability, the TMK plaintext is encrypted with a 3DES key preset by the TMS and the encrypted TMK is stored in a database of the TMS.

Additionally, a mark is defined at a message interface between the TMS and the POS terminal that indicates whether or not the TMK is required to be updated. In normal situations, the mark is set to be “no update is required”. When the POS terminal is required to update the TMK, an mark of “update is required” will be set in the message through the message interface by the TMS as long as any request, including check-in and transaction etc., is issued by the POS terminal to the TMS, and after the POS terminal has dealt with the normal responses sent by the TMS, if it is detected that the mark of “update is required” has become effective, then the update of the TMK is made so as to complete the automatic update of the TMK key. After completing the decrypt and storage of the TMK, the TMS replies to the POS terminal whether the TMK is successfully updated.

A bank card payment system for implementing the secure and automatic downloading of a master key is disclosed in the present invention, which includes a Point of Sale, a

Terminal Management System (TMS), a PIN PAD and a HSM, wherein the TMS invokes the HSM to generate a pair of public and private keys, wherein the private key is stored in the HSM and the public key is stored in a database of the TMS. The PIN PAD stores the public key downloaded from the TMS. The PIN PAD randomly generates the TMK master key and encrypts the TMK master key with the public key downloaded from the TMS. The HSM decrypts the TMK (the TMK is encrypted with the public key) with the private key, and stores the decrypted TMK, or encrypts the decrypted TMK using the 3DES encryption algorithm and stores it.

Additionally, a mark is defined in a message interface between the TMS and the POS terminal that indicates whether or not the TMK is required to be updated. When the POS terminal is required to update the TMK , an mark of "update is required" will be set in the message through the message interface by the TMS as long as any request, including check-in and transaction etc., is issued by the POS terminal to the TMS, and after the POS terminal has dealt with the normal responses sent by the TMS, if it is detected that the mark of "update is required" has become effective, then the update of the TMK is made so as to complete the automatic update of the TMK key; and in other normal situations, the mark is defined as "no update is required".

According to the present invention, the TMK is randomly generated, and the process of transmission is not exposed, and thus the TMK plaintext will not be exposed outside the secure storage devices, i.e., the PIN PAD and the HSM. The TMK remains encrypted with the public key during the entire process of transmission. The TMK cipher text can not be decrypted until it reaches the HSM of the TMS. Since the security level of such asymmetric encryption algorithm is high, the cipher text, even if being intercepted, will be difficult to be cracked, thus completely eliminating the security flaws that exist in the existing downloading processes of TMK.

Brief Description of the Drawings

Fig. 1 is a prior art procedure of downloading a working key;

Fig. 2 is a procedure of downloading a working key according to the present invention;

and

Fig. 3 is a procedure of updating the TMK according to the present invention.

Detailed Description

In order to overcome the defects of the existing TMK downloading methods stated above, a method for securely and automatically downloading the TMK is proposed in the present invention. The downloading of the TMK is centrally controlled and managed by the TMS. The data exchange with the POS terminals is done automatically. No human intervention is needed during the entire exchange process, thereby not only the cost of labor is dramatically decreased, but also the security and reliability of the TMK transmission is ensured .

To ensure the secure transmission of the TMK, an asymmetric encryption algorithm including public and private keys are introduced in the method. The concept of such encryption algorithm is: a pair of public and private keys are initially generated by the TMS invoking an HSM, wherein the private key is stored in an HSM and a public key is stored in the database of the TMS, the public key can be downloaded by the POS terminals. The flowchart of the downloading process is shown in Fig. 2, with the following steps:

A pair of public and private keys are generated by the TMS invoking an HSM, wherein the private key is stored in the HSM, and the public key is stored in the database of the TMS;

A request for downloading the public key is issued by the POS terminal;

The public key returned from the TMS is received by the POS terminal and stored in the PIN PAD.

In each of the TMK importing methods described above, the TMK is generated by the TMS, then is encrypted by certain encrypting means and transmitted to the POS terminals, and is decrypted by a corresponding decrypting means to obtain the TMK plaintext to be stored in the PIN PAD. However, advanced the encrypting means is, it cannot prevent a hacker or a internal personnel from intercepting the TMK plaintext with the same decrypting means.

In the design method proposed herein, a method of reversely generating the TMK is employed, with the detailed procedure as follows: a TMK is randomly generated in the PIN PAD by the POS terminal, and directly encrypted in the PIN PAD with a previously downloaded TMS public key, and then uploaded to the TMS, subsequently, is decrypted with the private key by the TMS invoking an HSM, and then the TMK plaintext is directly stored in the HSM, wherein during the entire process, the TMK plaintext will not be exposed outside the HSM. For those HSMs which do not store the TMK directly, the TMK will be encrypted by a 3DES key preset by the TMS before being stored into the database of the TMS. After aforementioned process, it can work closely with the existing key management system of the POS terminals, and is transparent to the subsequent processes of updating the PIK and MAK and encrypting the PIN, and thus no human intervention is needed. Steps of the procedure of updating the TMK in accordance with the present method are shown in Fig.3 and as follows:

A TMK is randomly generated by the POS terminal invoking the instructions provided by the PIN PAD, and is encrypted with the TMS's public key, and subsequently, is uploaded to the TMS;

The encrypted TMK is decrypted with the private key by the TMS invoking the HSM and then stored into the HSM. For those HSMs which do not store the TMK directly, the TMK will be encrypted by a 3DES key preset by the TMS before being stored into the database of the TMS for later use in the exchange of the PIK and MAK.

The TMS replys to the POS terminal whether or not the TMK is successfully updated.

As can be seen from the entire updating procedure described above, the TMK is randomly generated, and the transmission is not exposed, and thus the TMK plaintext will not be exposed outside the secure storage devices, i.e., the PIN PAD and the HSM. The TMK remains encrypted with the public key during the entire process of transmission. The TMK cipher text will not be decrypted until it reaches the HSM of the TMS. Since the security level of such asymmetric encryption algorithm is high, the cipher text, even if being intercepted, will be difficult to be cracked, thus completely eliminating the security flaws that exist in the existing processes of downloading TMK described above.

In order to implement such updating procedure that generates the TMK randomly, two

instructions need to be added to the existing PIN PAD, and the instructions are for:

1) storing the public key downloaded from the TMS; and

2) randomly generating the TMK key and encrypting it with the public key downloaded from the TMS.

One instruction is needed to be added to the HSM, and the instruction is for:

decrypting the TMK (the TMK is encrypted with the public key) with the private key and storing it, or decrypting the TMK and then re-encrypting it using 3DES encryption algorithm, and subsequently, storing it in the database of the TMS.

As can be seen from the TMK updating procedure described herein, the TMK updating procedure is initiated by the POS terminal, and an mark that indicates whether or not the TMK is required to be updated is defined in the message interface between the TMS and the POS terminal in order to meet the requirement of automatic management, and the mark is defined as follows:

1) no update is required;

2) update is required.

In a normal situation, wherein a TMK has been generated and in normal use and no update of the TMK is required, the mark is set to be “no update is required”. When the POS terminals (such as the newly installed POS terminal) is required to update the TMK, or the original TMK has expired, an mark of “update is required” will be set into the message through the message interface by the TMS as long as the POS terminal issues any request (including check-in and transaction etc.) to the TMS. After the normal response of the TMS has been handled by the POS terminal, if it is detected that the mark of “update is required” has become effective, then the updating procedure of the TMK will be automatically triggered to complete the automatic update of the TMK key. As can be seen, during the entire updating procedure of the TMK, all the control and management are completed in the TMS, and thus no human intervention is needed and no technical support personnel will be required to be sent to the site of the POS terminal to update the TMK. If in the “no update is required” state, the TMS receives a request for updating the TMK key issued by the POS terminal, it will directly reject the request, to prevent the information of the POS terminal from being copied or hijacked and being used in another POS terminal. In a case that the

POS terminal fails and does require to update the TMK key, the mark of the POS terminal will be set to be “update is required” by the TMS to allow the POS terminal to automatically complete the TMK updating procedure.

According to the method for securely and automatically downloading the TMK key described in the present invention, it is just required to add three simple instructions to the existing PIN PAD and HSM to meet the requirement of automatically downloading and secure management of the TMK. In this way, the security flaws of the existing TMK downloading procedure are avoided, and human intervention is reduced. Therefore, it is a secure, reliable, and effective method.

The advantages of the method are as follows: the asymmetric encryption algorithm, which is widely used and of high security level, is employed; it can be generally applied to the existing POS terminals and also to other automatic terminals with the similar key system, such as ATM terminals and payment terminals, etc; it is also of great commercial value and is worthy to be widely distributed.

CLAIMS

1. A method for securely and automatically downloading a master key TMK in a bank card payment system, wherein the bank card payment system includes a Point Of Sale POS, a Terminal Management system TMS, a PIN PAD, and a HSM, characterized in that the method comprises:

generating a pair of public and private keys by the TMS invoking the HSM;

randomly generating the master key TMK by the POS terminal invoking the PIN PAD;

encrypting the TMK with the public key of the TMS and uploading the encrypted TMK to the TMS; and

decrypting the TMK with the private key by the TMS invoking the HSM and storing the decrypted TMK.

2. A method of claim 1, characterized in that:

a pair of public and private keys are generated by the TMS invoking the HSM, wherein the private key is stored in the HSM and the public key is stored in a database of the TMS.

3. A method of claim 1, characterized in that:

a request for downloading the public key is initiated by the POS terminal; and

the public key returned from the TMS is received by the POS terminal and stored in the PIN PAD.

4. A method of claim 1, characterized in that:

the encrypted TMK is decrypted with the private key by the TMS invoking the HSM after the encrypted TMK is received from the POS terminal; and then

the TMK plaintext is directly stored in the HSM.

5. A method of claim 1, characterized in that:

the encrypted TMK is decrypted with the private key by the TMS invoking the HSM after the encrypted TMK is received from the POS terminal;

the TMK plaintext is encrypted with a 3DES key preset by the TMS; and then

the encrypted TMK is stored in the database of the TMS.

6. A method of claim 1, characterized in that:

a mark is defined in a message interface between the TMS and the POS terminal that indicates whether or not the TMK is required to be updated.

7. A method of claim 6, characterized in that:

when the POS terminal is required to update the TMK, the mark of "update is required" will be set in the message through the message interface by the TMS as long as any request, including check-in and transaction etc., is sent by the POS terminal to the TMS;

after the POS terminal has dealt with the normal responses of the TMS, if it is detected that the mark of "update is required" has become effective, then the TMK is updated according to claim 1, to complete the automatic update of the TMK key; and

in other normal situations, the mark is defined as "no update is required".

8. A method of claim 1, characterized in that:

after completing the decrypting and storing of the TMK, the TMS reply to the POS terminal whether the TMK is successfully updated.

9. A bank card payment system for implementing the secure downloading of a master key, including a Point of Sale POS, a Terminal Management System TMS, a PIN PAD and a HSM, characterized in that:

the TMS invokes the HSM to generate a pair of public and private keys, the PIN PAD stores the public key downloaded from the TMS, the PIN PAD randomly generates the TMK master key and encrypts the TMK master key with the public key downloaded from the TMS.

10. A system of claim 9, characterized in that:

the HSM decrypts the TMK with the private key, which TMK is encrypted with the public key, and then stores the decrypted TMK, or encrypts the decrypted TMK using the 3DES encryption algorithm and then stores it.

11. A system of claim 9, characterized in that:

the pair of public and private keys are generated by the TMS, wherein the private key is stored in the HSM and the public key is stored in a database of the TMS.

12. A system of claim 9, characterized in that:

a mark is defined in a message interface between the TMS and the POS terminal that indicates whether or not the TMK is required to be updated.

13. A system of claim 12, characterized in that:

when the POS terminal is required to update the TMK, the mark of "update is required"

will be set in the message through the message interface by the TMS as long as any request, including check-in and transaction etc., is sent by the POS terminal to the TMS; and

after the POS terminal has dealt with the normal responses of the TMS, if it is detected that the mark of “update is required” has become effective, then the automatic update of the TMK key is completed; and

in other normal situations, the mark is defined as “no update is required”.