

5

AUTHENTICATION SYSTEM AND METHOD**Field of the Invention**

This invention relates to an authentication system and method for enabling image-based mobile payment transactions. In particular, but not exclusively, the invention relates to a system and method when an image of a financial instrument or encrypted account number is used to initiate an orderlist or payment for goods and services as at least a part of the authentication system.

Background of the Invention

Electronic and mobile payment systems have been in use for some time, particularly for payments over the Internet. Payments using mobile telephony devices are in the process of evolving. Various methods of mobile payment methods are used for payment via SMS or MMS payments using inbuilt RFID. Many have problems with security and authentication. Quite often, complex systems are involved to provide security and authentication. Many such systems have not been a success, or even adopted, due to their inherent complexity and/or cost and/or inconvenience to users.

Summary of the Invention

In accordance with a first aspect, there is provided a method for authenticating a user for a payment transaction. The method comprises capturing a digital image of a representation forming a part of a financial instrument. The representation comprises an encrypted version of data pertaining to the user. The digital image is sent to a server for authentication of the user.

30

The data pertaining to the user may include a card number or account number in an encrypted image form.

The data pertaining to the user may also be compressed.

35

Authentication may comprise extracting from a key database, a key for the user; using the key to decrypt the representation and extract therefrom the data pertaining to the user; extracting identity information regarding the user from an

5 identity database, the identity information regarding the user comprising at least the data pertaining to the user; and comparing the identity information regarding the user and the data pertaining to the user for authentication of the user.

According to a second aspect, there is provided a method for authenticating a user
10 for a payment transaction. The method comprises receiving a message containing a digital image of a representation of encrypted version of data pertaining to the user. A key for user is extracted from a key database of encryption keys. The key is used to decrypt the representation to obtain the data pertaining to the user. Identity information regarding the user is extracted from an identity database. The
15 identity information regarding the user comprises at least the data pertaining to the user. The data pertaining to the user and the identity information regarding the user are compared to authenticate the user.

Preferably, the representation forms part of a financial instrument.

20

For both aspects the data pertaining to the user may be compressed. The data pertaining to the user may comprise at least one of: a number of the financial instrument, an expiry date of the financial instrument, the user's name, the user's date of birth, the user's address, and a photograph of the user's face. The financial
25 instrument may be a credit card, a debit card, internet banking card, prepaid card or a letter of credit. An authentication message may be sent to a financial institution, and an acknowledgement of authentication may also be sent.

The image may be captured using a mobile telephone with a digital camera, a
30 telecommunications enabled PDA with a digital camera, a digital camera able to be connected to a telecommunications enabled computer, a telecommunications enabled digital camera, and a web cam operatively connected to a computer. The digital image may be sent by MMS, SMS, email, instant message, digital data transfer and any other image transfer mechanism.

35

According to a third aspect there is provided a financial instrument for a payment transaction, the instrument comprising a representation comprising an encrypted version of data pertaining to a user. The data pertaining to the user may be compressed. The data pertaining to the user may comprise at least one of: a

- 5 number of the financial instrument, an expiry date of the financial instrument, the user's name, the user's date of birth, and the user's address, and a photograph of the user's face. The digital image may be sent by MMS, SMS, email, instant message, and digital data transfer.
- 10 The financial instrument may be one selected from the group consisting of: credit card, a debit card, a letter of credit, prepaid card, postpaid card, an account, virtual bank account, P2P payment instruments, a payment, receipt, and transfer of funds.

15 Accordingly to a final aspect there is provided a system for authenticating a user for a payment transaction, the system comprising a financial instrument containing a representation, the representation comprising an encrypted version of data pertaining to the user; an image capturing device for capturing a digital image of the representation; a server for:

- (i) receiving the digital image;
- 20 (ii) decrypting the representation to obtain the data pertaining to the user by using a key for the user extracted from a key database;
- (iii) extracting from an identity database identity information regarding the user; and
- (iv) comparing the identity information regarding the user with the data
- 25 pertaining to the user for authentication of the user.

Brief Description of the Drawings

In order that the invention may be fully understood and readily put into practical effect, there shall now be described by way of non-limitative example only a preferred embodiment of the present invention, the description being with reference

30 to the accompanying illustrative drawings in which:

Figure 1 is a schematic illustration of the system architecture;

Figure 2 is a schematic illustration of the server architecture; and

Figure 3 is a flow chart of the methodology.

35

Detailed Description of the preferred Embodiments

To first refer to Figure 1 there is shown a financial instrument 10 that is to be used to effect a financial transaction at a financial institution 18. The financial instrument

5 10 may be a credit card (as shown), debit card, letter of credit, prepaid card, postpaid card, an account, virtual bank account, P2P payment instruments, or other suitable financial instrument. The financial transaction may be a payment, receipt, transfer of funds, or the like.

10 The financial instrument 10 contains financial instrument data 11 relating to the owner, holder or user of the financial instrument 10. For example, and as shown for a credit card the financial instrument data 11 may be the account number 13 of the credit card, the expiry date 15 of the credit card, and the name 17 of the card holder.

15

The financial instrument 10 also includes a representation 19 containing an encrypted version of data pertaining to the user. The representation 19 may also be compressed. The data pertaining to the user may be one or more of: the financial instrument data 11, or any other data identifying or pertaining to the card holder. For example, the other data may include the date of birth of the card holder, a facial photograph of the card holder, biometric information, the address of the card holder, the maiden family name of the mother of the card holder, and so forth.

25 A tag or a digital image 9 of the representation 19 is captured using an image capturing device 12. The image capturing device 12 is capable of capturing a digital image 9 such as, for example, a digital camera, a mobile camera phone or PDA with a digital camera that is telecommunications enabled or can be operatively connected to a computer that is telecommunications enabled, a web-cam operatively connected to a computer that is telecommunications enabled and so forth. Capturing the tag initiates a mobile payment transaction. As part of the financial transaction, the image 9 of the representation 19 is sent to a server 20. The sending may be as digital data transfer, as an MMS message, as an SMS message, as an email or instant message, or otherwise as required or desired.

35 The methodology for sending the image 9 may depend on the nature of image capturing device 12.

The process of encryption and authentication for credit card based tags 19 is described as an example. Encryption of the tag 19 requires the financial institution 40 18 or card issuer to sign up and associate with a Tag Authentication Provider. The

5 Tag Authentication Provider generates a PKI key pair (RSA 1024 bytes key length) for the financial institution 18. Tag generation and encryption software is supplied to financial institution 18 or card issuer. This software is used to encrypt the credit card number, CVV number 13A, and expiration date of the card with the Private Key of the PKI key pair which is embedded in the software. The first six digits of the

10 card number or BIN number for uniquely identifying the financial institution 18 are left unencrypted in plain text form. The remaining digits of the card number, the CVV number 13A and expiration date are encrypted. The software converts this encrypted card information into a 25 slot tag 19. (4*25 matrix or 25 circular tags) sixteen for the credit card number; three for the CVV number 13A; and six for the

15 expiration date. This generated tag 19 is affixed or embedded onto the credit card.

Authentication for Credit Card Based Tags 19 requires capturing the customer's credit card tag 19 when receiving payment confirmation. In one embodiment, the customer sends the captured Tag 19 to the Tag Authentication Provider via MMS

20 through their camera-enabled mobile phone 12. The tag 19 is converted into a numerical format by a Tag Authentication Processor at the Tag Authentication Provider. The first six digits of the tag 19 are used to identify the Card Issuer or financial institution 18. The corresponding Public Key of the PKI key pair is used to decrypt the remaining credit card numbers, the CVV number 13A and expiration

25 date. This decrypted information is sent for authentication to the Card Issuer, financial institution 18 or Visa network. Subsequently, the appropriate amount is debited from the card by the card issuer.

From the server end, the server 20 receives, decrypts and attempts to match the

30 captured image with a corresponding image stored in an image database (not shown). The image database is connected to and communicates with the server 20. If the captured image is compressed, the server 20 decompresses the representation 19 in the image 9 to obtain the data pertaining to the user. This is used to authenticate the user, and the authentication can be passed to the financial

35 institution 18.

The server 20 has several modules. These include a processor 21 that receives the data of the image 9 from an inwards communication module 27. The processor 21 also communicates with a database controller 23 for extracting the necessary

40 key of the user for decryption from a key database 24 of such keys, and also information relative to the user from an identity database 25 of user identities. The

5 user identities contain at least the data pertaining to the user as encrypted and used for the representation 19. The processor 21 uses an authentication module 22 for authenticating the user by comparing the information relating to the user and the data pertaining to the user. If there is a sufficient match, there is authentication, otherwise there is no authentication. An outwards communications
10 module 26 is used to send an authentication code or message to the financial institution 18. The keys of the users are kept only in the database 24. Each financial instrument 10 will have a unique key. The unique key is generated randomly at the time of creation of the financial instrument 10 and is used to create the representation 19.

15

The flow is shown in Figure 3. Upon the payment transaction being initiated (31), the image 9 of representation 19 is captured (32) and send to server 20 (33). At server 20, the representation 19 is decrypted (34) using the correct user key extracted from database 24 and, if necessary, decompressed to obtain the data
20 pertaining to the user. Authentication then takes place (35) using the information relating to the user extracted from identity database 25.

The information relating to the user includes at least the data pertaining to the user. Authentication is performed by comparing the decrypted version of the data
25 pertaining to the user with the information relating to the user as obtained from the identity database 25. Upon authentication, an authentication code or message is sent to the financial institution 18 (37) and a confirmation is sent to the user (38). The authentication process then ends (39).

30 Whilst there has been described in the foregoing description preferred embodiments of the present invention, it will be understood by those skilled in the technology that many variations or modifications in details of design or construction or operation may be made without departing from the present invention.

5 **The Claims:**

1. A method for authenticating a user for a payment transaction, the method comprising:
 - (a) capturing a digital image of a representation forming a part of a financial instrument, the representation comprising an encrypted version of data pertaining to the user; and
 - (b) sending the digital image to a server for authentication of the user.
2. A method as claimed in claim 1, wherein the data pertaining to the user is compressed in the digital image
3. A method as claimed in claim 1, wherein the data pertaining to the user is compressed in the server.
4. A method as claimed in any one of claims 1 to 3, wherein the data pertaining to the user comprises at least one selected from the group consisting of: a number of the financial instrument, an expiry date of the financial instrument, the user's name, the user's date of birth, the user's address, and a photograph of the user's face.
5. A method as claimed in any one of the claims 1 to 4, wherein the financial instrument is selected from the group consisting of: credit card, debit card and letter of credit.
6. A method as claimed in any one of claims 1 to 5, wherein authentication comprises:
 - (a) extracting from a key database a key of the user;
 - (b) using the key to decrypt the representation and extracting therefrom the data pertaining to the user;
 - (c) extracting from an identity database identity information regarding the user, the identity information comprising at least the data pertaining to the user; and

- 5 (d) comparing the identity information and the data pertaining to the user for authentication of the user.
7. A method as claimed in any one of claims 1 to 7, further comprising sending an authentication message to a financial institution.
- 10
8. A method as claimed in any one of claims 1 to 7, further comprising sending an acknowledgement of authentication.
- 15
9. A method as claimed in any one of claims 1 to 8, wherein the image is captured using at least one of: a mobile telephone with a digital camera, a mobile camera phone, a telecommunications enabled PDA with a digital camera, a digital camera able to be connected to a telecommunications enabled computer, a digital camera able to be connected to a mobile telephone, a telecommunications enabled digital camera, and a web cam
- 20
- operatively connected to a computer.
10. A method as claimed in any one of claims 1 to 9, wherein the digital image is sent by one selected from the group consisting of: MMS, SMS, email, instant message, and digital data transfer.
- 25
11. A method for authenticating a user for a payment transaction, the method comprising:
- (a) receiving a message containing a digital image of a representation of encrypted version of data pertaining to the user;
- 30 (b) extracting from a key database of decryption keys a key for the user;
- (c) using the key to decrypt the representation to obtain the data pertaining to the user;
- 35 (d) extracting from an identity database identity information regarding the user, the identity information comprising at least the data pertaining to the user; and
- (e) comparing the data pertaining to the user and the identity information to authenticate the user.

5

12. A method as claimed in claim 11, wherein the representation forms part of a financial instrument.
13. A method as claimed in claim 11 or 12, wherein the data pertaining to the user is also compressed.
14. A method as claimed in claim 12 or claim 13, wherein the data pertaining to the user comprises at least one selected from the group consisting of: a number of the financial instrument, an expiry date of the financial instrument, the user's name, the user's date of birth, the user's address, and a photograph of the user's face.
15. A method as claimed in any one of the claims 12 to 14, wherein the financial instrument is selected from the group consisting of: credit card, debit card, and letter of credit.
16. A method as claimed in any one of claims 11 to 15, further comprising sending an authentication message to a financial institution.
17. A method as claimed in any one of claims 11 to 16, further comprising sending an acknowledgement of authentication.
18. A method as claimed in any one of claims 11 to 17, wherein the image is captured using at least one of: a mobile telephone with a digital camera, a telecommunications enabled PDA with a digital camera, a digital camera able to be connected to a telecommunications enabled computer, a telecommunications enabled digital camera, and a web cam operatively connected to a computer.
19. A financial instrument for a payment transaction, the instrument comprising a representation comprising an encrypted version of data pertaining to a user.

5

20. A financial instrument as claimed in claim 19, wherein the data pertaining to the user is also compressed.

10

21. A financial instrument as claimed in claim 19 or claim 20, wherein the data pertaining to the user comprises at least one selected from the group consisting of: a number of the financial instrument, an expiry date of the financial instrument, the user's name, the user's date of birth, the user's address, a photograph of the user's face.

15

22. A financial instrument as claimed in any one of claims 19 to 21, wherein the financial instrument is one selected from the group consisting of: credit card, a debit card, a letter of credit, prepaid card, postpaid card, an account, virtual bank account, P2P payment instruments, a payment, receipt, and transfer of funds.

20

23. A system for authenticating a user for a payment transaction, the system comprising:

25

(a) a financial instrument containing a representation, the representation comprising an encrypted version of data pertaining to the user;

(b) an image capturing device for capturing a digital image of the representation;

(c) a server for:

30

(i) receiving the digital image;

(ii) decrypting the representation to obtain the data pertaining to the user by using a key for the user extracted from a key database;

(iii) extracting from an identity database identity information regarding the user; and

35

(iv) comparing the identity information regarding the user with the data pertaining to the user for authentication of the user.

- 5 24. A method for authenticating a user for a payment transaction, the method comprising:

performing image recognition on a captured digital image to obtain authentication data, the captured digital image being a representation forming a part of a financial instrument, the representation comprising an encrypted version of data pertaining to the user;

10

processing the authentication data by decrypting the encrypted version of data pertaining to the user; and

transmitting the decrypted data to a server for authentication of the user and to effect payment of the transaction.

15

25. A method for producing a representation provided on a financial instrument for a payment transaction, the representation comprising an encrypted version of data pertaining to the user, the method comprising:

encrypting the data pertaining to the user with a private key of the Public Key Infrastructure (PKI) key pair, the encrypted data pertaining to the user including trailing identification numbers of the financial instrument, an anti-fraud number and expiration date of the financial instrument; and

20

converting the encrypted version of data pertaining to the user into a predetermined number of slots to define the representation.

25

26. The method according to claim 25, wherein the anti-fraud number is a Card Verification Value (CVV) number.

27. The method according to claim 25, wherein the trailing identification numbers are not a Bank Identification Number (BIN).
- 30

28. The method according to claim 25, wherein the slots are arranged in a matrix.

- 35 29. The method according to claim 25, wherein the slots are circular.