(12) STANDARD PATENT APPLICATION (11) Application No. **AU 2014202432 A1**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Payment Transaction Techniques

(51) International Patent Classification(s)
G06Q 20/30 (2012.01)

(21) Application No: **2014202432** (22) Date of Filing: **2014.05.05**

(30) Priority Data

(31) Number	(32) Date	(33) Country
2013901715	**2013.05.15**	**AU**

(43) Publication Date: **2014.12.04**
(43) Publication Journal Date: **2014.12.04**

(71) Applicant(s)
Julian Connop;Aidan Connop

(72) Inventor(s)
Connop, Aidan Daniel

(74) Agent / Attorney
Cullens Patent and Trade Mark Attorneys, GPO Box 1074, Brisbane, QLD, 4001

2014202432 05 May 2014

ABSTRACT

The present invention relates to a method for transacting payments. The method includes displaying a code, associated with a financial account and on a portable device, to be read when transacting payments with the account. Advantageously, the displayed code on the portable device can be conveniently read when transacting payments.

2014202432 05 May 2014

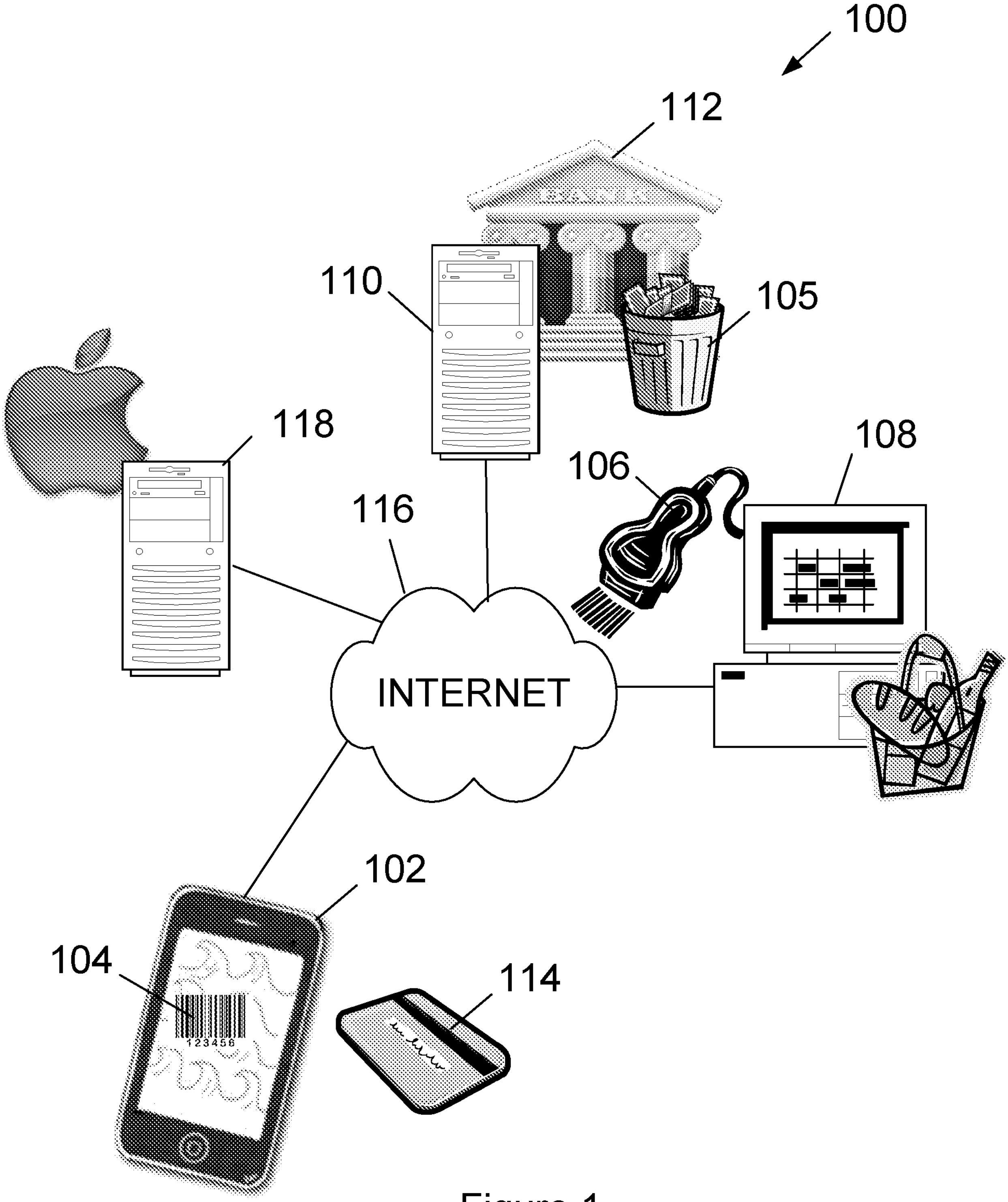

Figure 1

2014202432 05 May 2014

PAYMENT TRANSACTION TECHNIQUES

TECHNICAL FIELD

[0001] The present invention generally relates to a method for transacting payments.

BACKGROUND

[0002] The reference to any prior art in this specification is not, and should not be taken as an acknowledgement or any form of suggestion that the prior art forms part of the common general knowledge.

[0003] Financial cards, such as credit and debit cards, linked to financial accounts are a popular way to make payments when purchasing goods or services from suppliers. However, such cards are prone to fraudulent transactions, particularly online transactions in the event of cards being stolen and thieves gaining access to the associated account.

[0004] Furthermore, manual entry of card details during transactions is a laborious task often fraught with error.

[0005] The preferred embodiment provides for improved security and/or ease of financial card transactions.

SUMMARY OF THE INVENTION

[0006] According to one aspect of the present invention, there is provided a method for transacting payments including:

displaying a code, associated with a financial account and on a portable device, to be read when transacting payments with the account.

[0007] Advantageously, the displayed code on the portable device can be conveniently read when transacting payments. Preferably, the code is also associated with a financial (e.g. credit or debit) card. Preferably, the code is stored on the portable device so that the code can be displayed for reading irrespective of network connectivity of the device.

[0008] The method may further involve encryption to generate the code. The method may involve receiving, with the portable device, financial card details relating to the financial card and encrypting the details to generate the code. The financial card details may be manually typed into the device.

[0009] Encrypting may involve using a cryptographic key. Encrypting may involve encrypting a time stamp to set an expiry time beyond which payments cannot be made. The method may involve using format preserving encryption (FPE) so that the code is compact to ensure it fits on the display and to facilitate reading. Encrypting may involve the use of one-time pads to further increase security. Encrypting may involve storing a key on the device and updating the key over a network. Encrypting may involve sending encrypted card information to the device.

[00010] The code may include a token associated with the financial account.

[00011] The method may further involve displaying the code only after validating a personal identification number (PIN) entered into the portable device. The method may involve displaying a selectable image corresponding to the financial card, and displaying the code responsive to selection of the image.

[00012] The code may be a bar code or Quick Response (QR) code. The portable device may be a smart phone. The transacted payments may be made to or taken from the account.

[00013] According to another aspect of the present invention, there is provided a method for transacting payments including:

reading a code, associated with a financial account and displayed by a portable device, to transact payments with the account.

[00014] The read code may be encrypted and the method may further involve passing the read code, still in encrypted form, along to a financial provider server for processing payments. The financial provider server may decrypt the code and transact

2014202432 05 May 2014

payments from the associated financial account in accordance with received payment amounts.

[00015] The financial provider may receive a token associated with the financial account as authorization to transact payments. The financial provider may match tokens received from the device and a supplier server to authorize payments.

[00016] According to another aspect of the present invention, there is provided a portable device for use when transacting payments, the device configured to:

display a code, associated with a financial account and on a portable device, to be read when transacting payments with the account.

[00017] According to another aspect of the present invention, there is provided a supplier device for use in transacting payments, the device including:
a reader for reading a code, associated with a financial account and displayed by a portable device, to transact payments with the account.

[00018] According to another aspect of the present invention, there is provided a payment processing server for transacting payments, the server configured to:

receive a code, associated with a financial account and read by a supplier device when displayed by a portable device, to transact payments with the account.

[00019] According to another aspect of the present invention, there is provided a system for transacting payments, the system including:

a portable device for displaying a code, associated with a financial account, to be read when transacting payments with the account.

[00020] The system may further include a reader for reading the code. The system may further include a financial provider server for receiving the read code to transact payments with the account.

[00021] Any of the features described herein can be combined in any combination with any one or more of the other features described herein within the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[00022] Preferred features, embodiments and variations of the invention may be discerned from the following Detailed Description which provides sufficient information for those skilled in the art to perform the invention. The Detailed Description is not to be regarded as limiting the scope of the preceding Summary of the Invention in any way. The Detailed Description will make reference to a number of drawings as follows:

[00023] Figure 1 is a schematic drawing of a payment transaction system in accordance with an embodiment of the present invention;

[00024] Figure 2 is a flowchart showing a payment transaction method performed using the system of Figure 1.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[00025] According to an embodiment of the present invention, there is provided a payment transaction system 100 as shown in Figure 1. The system 100 includes a portable smart phone device 102 for displaying a common image code 104, associated with a financial (e.g. bank) account 105, to be read when transacting multiple payments with the account 105.

[00026] The system 100 further includes a supplier reader 106 in the form of a handheld scanner for reading the code 104. A grocery supplier computer 108 interfaces to a financial server 110 of a financial provider (e.g. bank) 112 that issues a financial (e.g. credit or debit) card 114 associated with the financial account 105. The supplier computer 108 typically includes the scanner reader 106 and the supplier would not need to purchase any additional hardware. . The financial server 110 receives the read code 104 via the internet 116 to transact payments to and from the account 105.

[00027] The system 100 further includes an Application software (i.e. App) sales server 118 from which a payment transaction App can be purchased and downloaded to the device 102 for execution.

[00028] According to one embodiment of the present invention, there is provided a payment transaction method 200 shown in Figure 2 which is performed using the system 100.

[00029] Initially, at step 202, the device 102 downloads the payment transaction App from the App sales server 118.

[00030] At step 204, the device 102 receives financial card details (e.g. credit card number, expiry date, etc.) relating to the financial card 114. The financial card details are manually typed into the device using a touch screen keypad.

[00031] At step 206, the device 102 executing the App generates the barcode 104 by encrypting the entered financial card details. The card details are no longer visible to the device user and a key is required to decrypt the code. The code 104 can include an encrypted time stamp to set an expiry time (e.g. two hours from code creation) beyond which payments cannot be made.

[00032] At step 208, the device 102 locally stores the barcode 104 on internal non-volatile memory and associates the code 104 with a pictorial image of the card 114. Similarly, the device102 stores other barcodes 104 associated with other cards 114. The codes 104 are stored on the portable device 102 in non-volatile memory so that the code 104 can be displayed for reading during purchasing, irrespective of network connectivity of the device 102.

[00033] At step 210, when later making a grocery purchase, the device 102 validates a personal identification number (PIN) typed into the portable device. The PIN may be associated with either the App or firmware of the device 102 itself.

[00034] At step 212, upon validation, the device 102 displays the selectable pictorial image corresponding to the financial card 114, along with other pictorial images corresponding to other stored cards 114. The pictorial images can be customized by the device user for easy recognition. The credit card images can be scrolled on the screen in number.

[00035] At step 214 responsive to selection of the pictorial image using the touch screen, the device 102 displays the code 104 associated with the financial account 105.

[00036] At step 216, the supplier reader 106 reads the displayed code 104 on the device 102 to transact payments with the account 105. The transacted payments may be taken from the electronic account 105 when purchasing groceries or deposited into the account when returning groceries.

[00037] At step 218, the read encrypted code is passed in encrypted form along to the financial provider server 110 for processing the grocery payment. The financial provider server 110 decrypts the code 104, and takes payment for the groceries from the associated financial account 105 in accordance with a received payment amount (e.g. $50) from the grocery supplier computer 108.

[00038] At step 220, the device 102 ceases displaying the code 104. The same code 104 can be once again displayed on device 102 when making other purchases and associated payments from step 210.

[00039] Advantageously, the foregoing method 200 requires no communication between the device 102 and the financial provider server 110 and therefore a payment transaction is possible even in remote locations when the smart phone device 102 does not have network reception or coverage. The method 200 provides for improved security of credit card transactions, particularly given that the code 104 is displayed responsive to the correct PIN first being entered. Further, the user need not carry financial cards around and can instead simply use their phone device 102 to conveniently and efficiently make purchases, irrespective of whether the phone device 102 is near field chip (NFC) enabled.

[00040] There are variations to the type of encryption used, and symmetric and asymmetric encryption can be used.

[00041] In a symmetric encryption scheme, the key used to encrypt and decrypt card details is the same.

[00042] In an asymmetric encryption scheme, there is private and public keys. The private key can decrypt card details whereas the public key can encrypt card details only.

[00043] In one embodiment, the mobile device 102 utilises asymmetric encryption and has a copy of the public key accessible by the payment App allowing it to encrypt but not decrypt card data. The payment processing server 110 for making the payment transaction possess the private key and so is able to decrypt the card data and use it for payment. However when information is encrypted, the resulting ciphertext can be much longer and in a different format to the original unencrypted plaintext. Undesirably, the bar code 104 becomes much too large to be able to be displayed on a screen of the mobile device 102 or to be read by a standard barcode scanner 106. A QR code and scanner would be an acceptable alternative in this embodiment.

[00044] In another embodiment, Format Preserving Encryption (FPE) can be used. Using FPE advantageously ensures that the encrypted ciphertext remains of the same data type and length as the original plaintext. However, traditionally, FPE utilizes symmetric encryption only. In order to use encryption in the payment App, it is desirous that FPE for the code 104 fits on mobile device screen and is able to be scanned, but preferably the key is not stored locally on the device 102.

[00045] Two possible encryption alternatives include:

1. The cryptographic key is stored on the device 102 and by using the device's internet connection, periodically at set intervals a new key is issued from the payment processing server 110 to the device 102 to maintain security, reducing the chance of the key being deciphered.
2. When details of a new card 114 are entered into the App, the App sends associated unencrypted data over a secure connection to a server 110 without storing the card data. The server 110 possesses the key, and encrypts the card 114 for the device 102 and sends back the encrypted code 104 to the device 102 without storing the unencrypted card data. A key rotation scheme can also be used to improve security.

[00046] The second solution may be preferred, as neither the key nor the unencrypted card data is stored on the mobile device 102. Also, the unencrypted card data is not stored on the Server 110 providing the encrypting service. Only the mobile device 102 has a copy of the encrypted card data or code 104 which can only be decrypted by the Server 110 having possession of the key.

[00047] Another embodiment makes use of tokens, which are essentially substitutions, for improved security. A card's information can be stored securely by the Payment processing server 110 along with a token representing the card 114, account 105 and the associated end user. When the end user makes a payment, the token is presented as a bar code 104. The token can be just an account number for example. The Server 110 receiving the token from the supplier computer 108 matches the token to the read card information and processes the payment.

[00048] Once again, the same common bar code 104 representing the token can be used for making numerous payments and does not require the mobile device 102 to be connected to the payment processing server 110 via internet 116 to successfully complete a transaction.

[00049] In yet another embodiment, the two systems of encryption and tokenization could be used together. Upon downloading the App to device 102, the user registers with the server 110 which generates a token for later use. The server 110 maintains a database of users and their associated tokens. The user enters their card data into the device 102, which is encrypted with a public key and saved on the device 102.

[00050] When a sale is made, the device 102 displays a bar code 104 representing the token, and the supplier computer 108 passes the read code 104 along with the payment amount to the payment processing server 110 along with a time stamp. The server 110, receiving the foregoing, registers that the end user intends making a payment and begins to count down a predetermined time window for a payment.

[00051] The mobile device 102 after having the code 104 scanned by the computer 108 sends to the server 110 over the internet 116 its token and the encrypted code 104. The server 110 then matches the codes 104 representing tokens from the user's device 102 and the supplier computer 108, decrypts the code 104 and processes the transaction.

[00052] A person skilled in the art will appreciate that many embodiments and variations can be made without departing from the ambit of the present invention.

[00053] For example, the code 104 may be a two-dimensional quick response (QR) code. The portable device 102 may be a tablet, personal digital assistant or other like networked device.

[00054] In one embodiment, the payment processing server 110 of the "payment gateway" may be administered by a party other than an issuer of financial cards 114.

[00055] Another embodiment makes use of a variation of a one-time pad (OTP) to further increase security of the system as a whole, as explained below.

[00056] A one-time pad is a method of encryption where the sending and receiving parties both retain a list of codes used to encrypt the data or message. The codes are created using randomly chosen numbers or characters. Each transmission uses the next available code in the list, or pad and is subsequently deleted from the list after transmission. If the numbers or characters used to generate the encrypted code are truly random it is computationally impossible to break the encryption without a current copy of the Pad.

[00057] At step 206 when the server 110 is encrypting the card data 114 a list of randomly generated numbers is also created, forming the OTP and containing as many entries as deemed necessary, perhaps several hundred to thousand lines long.

[00058] As the entries must be appended to the encrypted card code, each entry could be limited for instance to four digit numbers thus keeping the overall length of the code within practical length for display as a bar code.

[00059] The OTP is transmitted to the device 102 along with the encrypted card data, with the server 110 also retaining a copy of this same list along with the encrypted card data enabling it to later reference cards to OTP lists.

[00060] Each OTP is individual to each stored card and generated at the time of card encryption.

[00061] At step 214, the code is displayed along with the next entry in the OTP, together forming a single bar code, the OTP entry being deleted after each use.

[00062] The server 110, when receiving the code and OTP entry, matches the code and OTP entry within its own database and confirms a match. If the match is successful the server 110 processes the payment and deletes the entry from its own OTP.

[00063] A further embodiment uses a one-time pad (OTP) in its traditional sense, as explained below.

[00064] At step 206, when the server 110 is encrypting the card data 114, an OTP is generated and used to encrypt the card data multiple times creating a list, or 'pad' with as many entries as is deemed necessary. The OTP out of necessity is paired with a Token to identify OTP's with individual cards.

[00065] Each OTP and Token is individual to each stored card and generated at the time of card encryption.

[00066] The OTP and Token are transmitted to the device 102 over a secure connection for later use, with the server 110 also retaining a copy of this same OTP along with the Token.

[00067] At step 214, the code displayed is comprised of the top entry of the OTP and the Token.

[00068] The server 110, when receiving the code, compares the code to its own database and confirms a match. If the match is successful the server 110 processes the payment and deletes the entry from its own copy of the OTP.

[00069] As there is scope for the one-time pad's to lose synchronicity between the device 102 and the server 110, for instance if a transaction is cancelled before the code is read, further checks must be in place to prevent failures.

[00070] One practical solution is for the server 110 to accept any entry from the top several entries (for example 5) from a particular referenced Token or Card. This would allow for several cancelled or failed transactions without preventing a successful transaction on the next attempt. The App would after each transaction attempt to make a secure connection to the server 110 over the internet where it would perform a synchronisation of the OTP's. In the instance an Internet connection is not available, the system would rely on the server's ability to accept an entry from the devices OTP that is not necessarily from the top of the Pad.

[00071] In compliance with the statute, the invention has been described in language more or less specific to structural or methodical features. It is to be understood that the invention is not limited to specific features shown or described since the means herein described comprises preferred forms of putting the invention into effect.

[00072] Reference throughout this specification to 'one embodiment' or 'an embodiment' means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearance of the phrases 'in one embodiment' or 'in an embodiment' in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more combinations.

The claims defining the invention are as follows:

1. A method for transacting payments including:

displaying a code, associated with a financial account and on a portable device, to be read when transacting payments with the account.

2. A method as claimed in claim 1, wherein the code is also associated with a financial card.

3. A method as claimed in claim 1 or claim 2, wherein the code is stored on the portable device so that the code can be displayed for reading irrespective of network connectivity of the device.

4. A method as claimed in any one of the preceding claims, further involving encryption to generate the code.

5. A method as claimed in claim 4, further involving receiving, with the portable device, financial card details relating to the financial card and encrypting the details to generate the code.

6. A method as claimed in claim 5, wherein the financial card details can be manually typed into the device.

7. A method as claimed in any one of claims 4 to 6, wherein the encryption involves using a cryptographic key or one-time pads.

8. A method as claimed in any one of claims 4 to 7, wherein the encryption involves encrypting a time stamp to set an expiry time beyond which payments cannot be made.

9. A method as claimed in any one of claims 4 to 8, wherein the encryption involves using format preserving encryption (FPE) so that the code is compact to ensure it fits on the display and to facilitate reading.

10. A method as claimed in any one of claims 4 to 9, wherein the encryption involves storing a key on the device and updating the key over a network.

11. A method as claimed in any one of claims 4 to 10, wherein the encryption involves sending encrypted card information to the device.

12. A method as claimed in any one of the preceding claims, wherein the code includes a token associated with the financial account.

13. A method as claimed in any one of the preceding claims, further involving displaying the code only after validating a personal identification number (PIN) entered into the portable device.

14. A method as claimed in any one of the preceding claims, further involving displaying a selectable image corresponding to the financial card, and displaying the code responsive to selection of the image.

15. A method for transacting payments including:

reading a code, associated with a financial account and displayed by a portable device, to transact payments with the account.

16. A method as claimed in claim 15, wherein the read code is encrypted and the method further involves passing the read code, still in encrypted form, along to a financial provider server for processing payments.

17. A method as claimed in claim 15 or claim 16, wherein a financial provider server decrypts the code and transacts payments from the associated financial account in accordance with received payment amounts.

18. A method as claimed in any one of claims 15 to 17, wherein a financial provider server receives a token associated with the financial account as authorization to transact payments.

19. A method as claimed in any one of claims 15 to 18, wherein a financial provider server matches tokens received from the device and a supplier server to authorize payments.

20. A portable device for use when transacting payments, the device configured to:

display a code, associated with a financial account and on a portable device, to be read when transacting payments with the account.

21. A supplier device for use in transacting payments, the device including:

a reader for reading a code, associated with a financial account and displayed by a portable device, to transact payments with the account.

22. A payment processing server for transacting payments, the server configured to:

receive a code, associated with a financial account and read by a supplier device when displayed by a portable device, to transact payments with the account.

23. A system for transacting payments, the system including:

a portable device for displaying a code, associated with a financial account, to be read when transacting payments with the account.

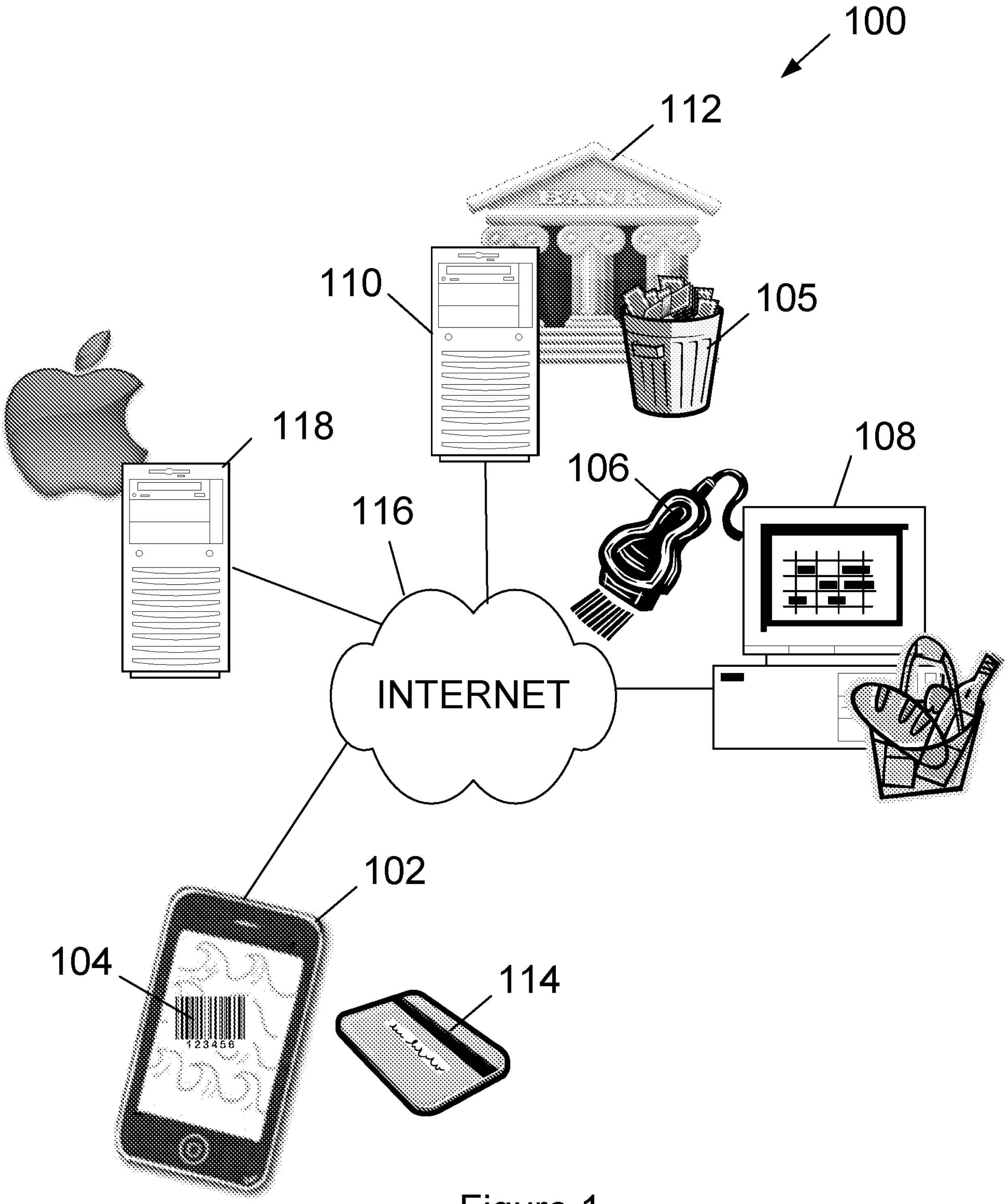

Figure 1

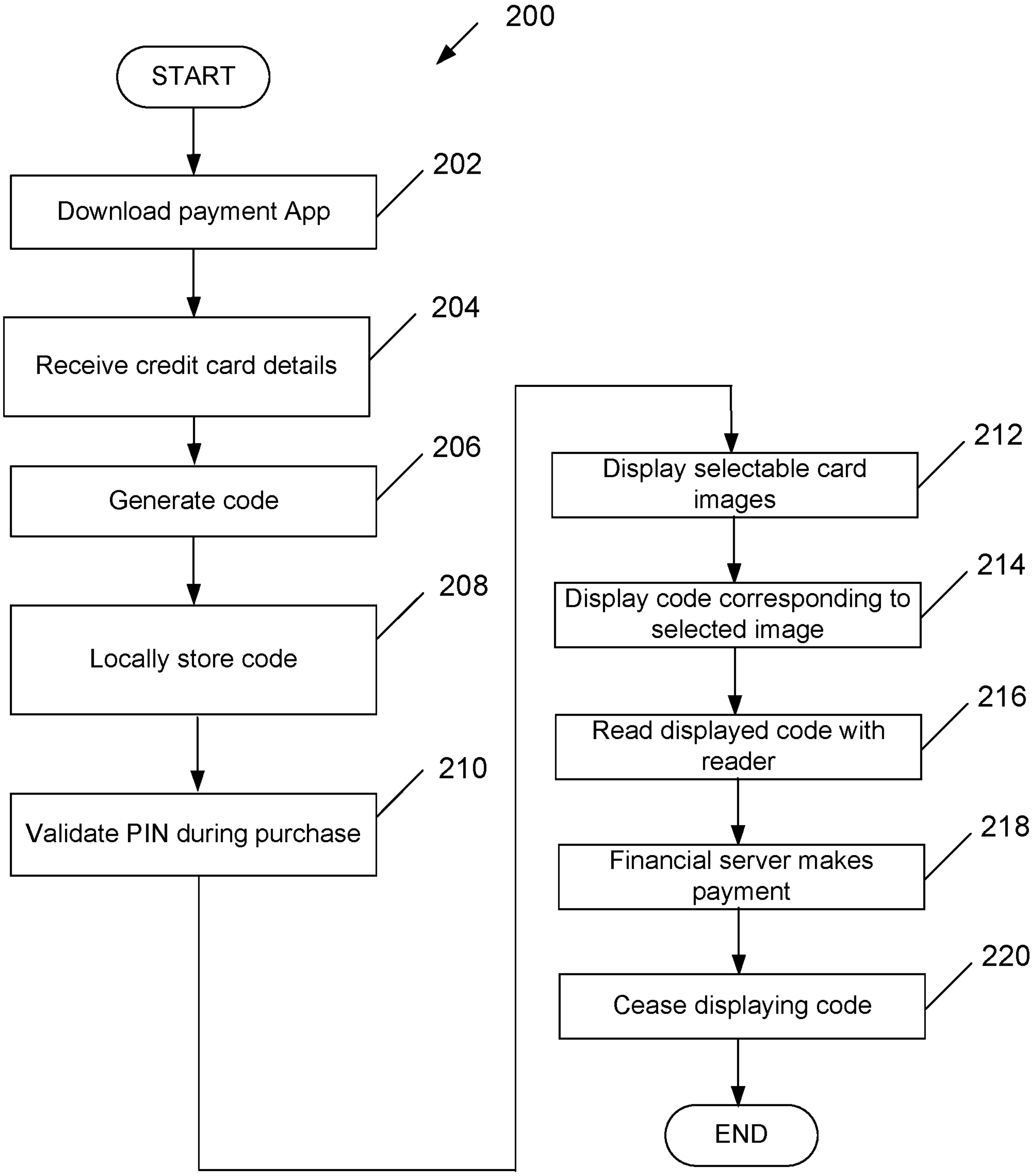
200
START
Download payment App
202
Receive credit card details
204
Generate code
206
Locally store code
208
Validate PIN during purchase
210
Display selectable card images
212
Display code corresponding to selected image
214
Read displayed code with reader
216
Financial server makes payment
218
Cease displaying code
220
END

Figure 2