



US009015064B2

(12) **United States Patent**
Fisher

(10) **Patent No.:** **US 9,015,064 B2**

(45) **Date of Patent:** ***Apr. 21, 2015**

(54) **UTILIZING A SECURE ELEMENT FOR NFC TRANSACTIONS WHICH INCLUDES RESPONSE DATA DURING INDUCTION**

USPC 455/406, 410, 558, 41.1, 556.1; 705/16, 705/18, 30, 40, 41, 44, 5, 51, 64; 235/462.42, 462.11, 380-385, 451
See application file for complete search history.

(71) Applicant: **Blaze Mobile, Inc.**, Berkeley, CA (US)

(72) Inventor: **Michelle Fisher**, Oakland, CA (US)

(73) Assignee: **Michelle Fisher**, Marina del Rey, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 13 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/710,646**

(22) Filed: **Dec. 11, 2012**

(65) **Prior Publication Data**

US 2013/0097032 A1 Apr. 18, 2013

Related U.S. Application Data

(63) Continuation of application No. 11/948,903, filed on Nov. 30, 2007, now Pat. No. 8,352,323.

(51) **Int. Cl.**

G06Q 20/00 (2012.01)

G06F 21/00 (2013.01)

(Continued)

(52) **U.S. Cl.**

CPC **G06Q 20/322** (2013.01); **G06Q 20/105** (2013.01); **G06Q 20/10** (2013.01);

(Continued)

(58) **Field of Classification Search**

CPC ... G06Q 20/20; G06Q 20/206; G06Q 20/102; G06Q 20/105; G06Q 40/10; G06Q 20/327; G06Q 20/341; G06Q 20/3552; G06Q 20/045; H04W 12/12; H04W 4/24; H04M 1/725; H04M 1/72

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,038,367 A 3/2000 Abecassis
6,101,483 A * 8/2000 Petrovich et al. 705/21

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 2006095212 A1 9/2006
WO WO 2006095212 A1 * 9/2006 H04M 11/00

OTHER PUBLICATIONS

Editors, B. (Sep. 5, 2002). Philips and sony announce strategic cooperation to define next generation near field radio-frequency communications. Business Wire Retrieved from <http://search.proquest.com/docview/444976968?accountid=14753>.*

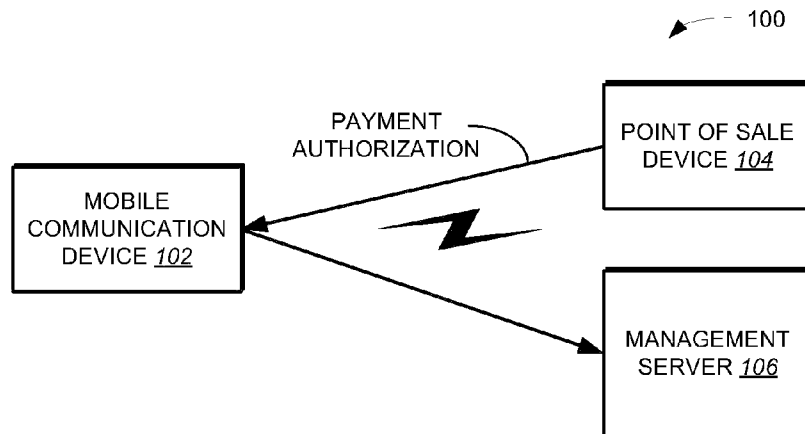
(Continued)

Primary Examiner — Olusegun Goyea

(57) **ABSTRACT**

A method and system for conducting an online payment transaction through a point of sale device. The method includes receiving input from a user selecting an item for purchase through the point of sale device; calculating a total purchase amount for the item in response to a request from the user to purchase the item; and sending payment authorization for the total purchase amount from the point of sale device to a payment entity, in which the payment authorization is sent to the payment entity via a mobile communication device of the user. The method further includes receiving a result of the payment authorization from the payment entity through the mobile communication device; and completing the payment transaction based on the result of the payment authorization.

21 Claims, 4 Drawing Sheets



(51) **Int. Cl.**

<i>H04M 11/00</i>	(2006.01)	7,069,248 B2	6/2006	Huber	
<i>G06K 5/00</i>	(2006.01)	7,096,003 B2	8/2006	Joao	
<i>G06K 15/00</i>	(2006.01)	7,110,744 B2	9/2006	Freeny	
<i>G06Q 20/32</i>	(2012.01)	7,110,792 B2*	9/2006	Rosenberg	455/558
<i>G06Q 20/20</i>	(2012.01)	7,127,236 B2	10/2006	Khan	
<i>G06Q 30/02</i>	(2012.01)	7,200,578 B2*	4/2007	Paltenghe et al.	705/74
<i>G06Q 30/06</i>	(2012.01)	7,289,810 B2	10/2007	Jagadeesan	
<i>G06Q 20/38</i>	(2012.01)	7,308,254 B1	12/2007	Rissanen	
<i>G06Q 20/40</i>	(2012.01)	7,357,312 B2	4/2008	Gangi	
<i>G06Q 20/36</i>	(2012.01)	7,379,920 B2	5/2008	Leung	
<i>G06Q 20/16</i>	(2012.01)	7,472,829 B2	1/2009	Brown	
<i>G06Q 40/00</i>	(2012.01)	7,482,925 B2	1/2009	Hammad	
<i>H04W 4/20</i>	(2009.01)	7,512,567 B2*	3/2009	Bemmel et al.	705/67
<i>H04W 8/20</i>	(2009.01)	7,522,905 B2	4/2009	Hammad	
<i>H04M 1/725</i>	(2006.01)	7,784,684 B2*	8/2010	Labrou et al.	235/380
<i>H04W 4/18</i>	(2009.01)	7,870,077 B2*	1/2011	Woo et al.	705/78
<i>G06Q 20/10</i>	(2012.01)	7,946,493 B2*	5/2011	Havens et al.	235/462.42
<i>H04N 21/81</i>	(2011.01)	7,979,519 B2*	7/2011	Shigeta et al.	705/223
<i>G07F 7/10</i>	(2006.01)	8,005,426 B2*	8/2011	Huomo et al.	455/41.2
<i>H04W 88/02</i>	(2009.01)	8,019,362 B2*	9/2011	Sweatman et al.	455/466
<i>H04W 4/02</i>	(2009.01)	8,073,424 B2*	12/2011	Sun et al.	455/406
		8,086,534 B2*	12/2011	Powell	705/44
		8,109,444 B2*	2/2012	Jain	235/492
		8,121,945 B2	2/2012	Rackley	
		8,127,984 B2*	3/2012	Zatloukal et al.	235/380
		8,214,454 B1*	7/2012	Barnes et al.	709/217
		8,261,992 B2*	9/2012	Havens et al.	235/462.42
		2001/0011250 A1*	8/2001	Paltenghe et al.	705/41
		2001/0044751 A1*	11/2001	Pugliese et al.	705/26
		2002/0056091 A1*	5/2002	Bala et al.	725/34

(52) **U.S. Cl.**

CPC *G06Q 20/20* (2013.01); *G06Q 20/32* (2013.01); *G06Q 20/3278* (2013.01); *G06Q 30/0222* (2013.01); *G06Q 30/06* (2013.01); *G06Q 30/0238* (2013.01); *G06Q 30/02* (2013.01); *G06Q 20/3821* (2013.01); *H04W 4/008* (2013.01); *G06Q 20/409* (2013.01); *G06Q 20/202* (2013.01); *G06Q 20/3226* (2013.01); *G06Q 20/3674* (2013.01); *G06Q 20/3227* (2013.01); *G06Q 20/40* (2013.01); *G06Q 20/16* (2013.01); *G06Q 20/4012* (2013.01); *G06Q 20/206* (2013.01); *G06Q 20/00* (2013.01); *G06Q 40/10* (2013.01); *H04N 21/812* (2013.01); *G07F 7/1008* (2013.01); *G06Q 20/108* (2013.01); *G06Q 20/4014* (2013.01); *G06Q 20/204* (2013.01); *G06Q 40/00* (2013.01); *G06Q 20/325* (2013.01); *G06Q 30/0253* (2013.01); *G06Q 30/0613* (2013.01); *H04W 4/206* (2013.01); *H04W 8/205* (2013.01); *H04W 88/02* (2013.01); *G06Q 30/0267* (2013.01); *G06Q 20/3223* (2013.01); *G06Q 30/0268* (2013.01); *H04M 1/72561* (2013.01); *H04W 4/02* (2013.01); *H04W 4/18* (2013.01); *G06Q 30/0251* (2013.01); *G06Q 30/0635* (2013.01)

2002/0059100 A1	5/2002	Shore	
2002/0063895 A1	5/2002	Agata	
2002/0065774 A1*	5/2002	Young et al.	705/41
2002/0077918 A1	6/2002	Lerner	
2002/0082879 A1	6/2002	Miller	
2002/0107756 A1	8/2002	Hammons	
2002/0116269 A1*	8/2002	Ishida	705/14
2002/0160761 A1*	10/2002	Wolfe	455/414
2002/0169984 A1	11/2002	Kumar	
2003/0061113 A1*	3/2003	Petrovich et al.	705/26
2003/0065805 A1	4/2003	Barnes	
2003/0074259 A1*	4/2003	Slyman et al.	705/14
2003/0085286 A1*	5/2003	Kelley et al.	235/492
2003/0087601 A1*	5/2003	Agam et al.	455/39
2003/0093695 A1	5/2003	Dutta	
2003/0105641 A1	6/2003	Lewis	
2003/0132298 A1*	7/2003	Swartz et al.	235/472.02
2003/0140004 A1	7/2003	O'Leary	
2003/0144793 A1*	7/2003	Melaku et al.	701/209
2003/0163359 A1*	8/2003	Kanesaka	705/8
2003/0172028 A1	9/2003	Abell	
2004/0006497 A1	1/2004	Nestor	
2004/0030658 A1	2/2004	Cruz	
2004/0034544 A1	2/2004	Fields	
2004/0073497 A1*	4/2004	Hayes et al.	705/27
2004/0127256 A1*	7/2004	Goldthwaite et al.	455/558
2004/0235450 A1*	11/2004	Rosenberg	455/406
2004/0243519 A1	12/2004	Perttila	
2004/0249710 A1*	12/2004	Smith et al.	705/14
2004/0254836 A1*	12/2004	Emoke Barabas et al.	705/14
2004/0267618 A1	12/2004	Judicibus	
2004/0267665 A1	12/2004	Nam	
2005/0003810 A1	1/2005	Chu	
2005/0040230 A1*	2/2005	Swartz et al.	235/383
2005/0076210 A1	4/2005	Thomas	
2005/0187873 A1*	8/2005	Labrou et al.	705/40
2005/0215231 A1	9/2005	Bauchot	
2006/0031752 A1*	2/2006	Surloff et al.	715/501.1
2006/0087474 A1*	4/2006	Do et al.	342/386
2006/0089874 A1*	4/2006	Newman et al.	705/14
2006/0143091 A1*	6/2006	Yuan et al.	705/26
2006/0191995 A1*	8/2006	Stewart et al.	235/379
2006/0197753 A1*	9/2006	Hotelling	345/173
2006/0206709 A1*	9/2006	Labrou et al.	713/167
2006/0219780 A1*	10/2006	Swartz et al.	235/383
2006/0287920 A1*	12/2006	Perkins et al.	705/14
2007/0004391 A1	1/2007	Maffeis	
2007/0011099 A1*	1/2007	Sheehan	705/65
2007/0022058 A1*	1/2007	Labrou et al.	705/67

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,115,601 A *	9/2000	Ferreira	455/406
6,123,259 A *	9/2000	Ogasawara	235/380
6,128,655 A	10/2000	Fields	
6,141,666 A	10/2000	Tobin	
6,199,082 B1	3/2001	Ferrel	
6,250,557 B1*	6/2001	Forslund et al.	235/492
6,415,156 B1	7/2002	Stadelmann	
6,450,407 B1*	9/2002	Freeman et al.	235/492
6,587,835 B1*	7/2003	Treyz et al.	705/14.64
6,605,120 B1	8/2003	Fields	
6,771,981 B1	8/2004	Zalewski	
6,772,396 B1	8/2004	Cronin	
6,886,017 B1	4/2005	Jackson	
6,950,939 B2	9/2005	Tobin	
7,031,945 B1	4/2006	Donner	

(56)

References Cited

U.S. PATENT DOCUMENTS

2007/0095892 A1 5/2007 Lyons
 2007/0125838 A1* 6/2007 Law et al. 235/379
 2007/0125840 A1* 6/2007 Law et al. 235/379
 2007/0131759 A1* 6/2007 Cox et al. 235/380
 2007/0138299 A1* 6/2007 Mitra 235/492
 2007/0156436 A1* 7/2007 Fisher et al. 705/1
 2007/0210155 A1* 9/2007 Swartz et al. 235/383
 2007/0235519 A1 10/2007 Jang
 2007/0255662 A1 11/2007 Tumminaro
 2007/0270166 A1* 11/2007 Hampel et al. 455/456.3
 2007/0293155 A1* 12/2007 Liao et al. 455/41.2
 2008/0010190 A1 1/2008 Rackley
 2008/0010196 A1* 1/2008 Rackley, III et al. 705/40
 2008/0017704 A1* 1/2008 VanDeburg et al. 235/380
 2008/0045172 A1* 2/2008 Narayanaswami et al. 455/187.1
 2008/0046366 A1 2/2008 Bommel
 2008/0048022 A1* 2/2008 Vawter 235/380
 2008/0051059 A1* 2/2008 Fisher 455/410
 2008/0051142 A1* 2/2008 Calvet et al. 455/558
 2008/0052192 A1* 2/2008 Fisher 705/26
 2008/0052233 A1* 2/2008 Fisher et al. 705/40
 2008/0088602 A1* 4/2008 Hotelling 345/173
 2008/0139155 A1 6/2008 Boireau
 2008/0148040 A1* 6/2008 Machani et al. 713/150
 2008/0167988 A1* 7/2008 Sun et al. 705/39
 2008/0177668 A1 7/2008 Delean
 2008/0207234 A1* 8/2008 Arthur et al. 455/466
 2008/0208681 A1 8/2008 Hammad
 2008/0208743 A1* 8/2008 Arthur et al. 705/41
 2008/0208744 A1* 8/2008 Arthur et al. 705/41
 2008/0208762 A1* 8/2008 Arthur et al. 705/79
 2008/0221997 A1* 9/2008 Wolfe 705/14
 2008/0255947 A1* 10/2008 Friedman 705/14
 2008/0262928 A1* 10/2008 Michaelis 705/14
 2008/0275779 A1* 11/2008 Lakshminarayanan 705/14
 2008/0294556 A1 11/2008 Anderson
 2008/0305774 A1 12/2008 Ramakrishna
 2009/0063312 A1* 3/2009 Hurst 705/30
 2009/0088203 A1* 4/2009 Havens et al. 455/556.1
 2009/0090783 A1* 4/2009 Killian et al. 235/492
 2009/0094123 A1* 4/2009 Killian et al. 705/16
 2009/0094125 A1* 4/2009 Killian et al. 705/17
 2009/0094126 A1* 4/2009 Killian et al. 705/17
 2009/0098825 A1* 4/2009 Huomo et al. 455/41.1
 2009/0104888 A1* 4/2009 Cox 455/410
 2009/0106112 A1* 4/2009 Dalmia et al. 705/14

2009/0124234 A1* 5/2009 Fisher et al. 455/406
 2009/0132362 A1* 5/2009 Fisher et al. 705/14
 2009/0143104 A1* 6/2009 Loh et al. 455/558
 2009/0144161 A1* 6/2009 Fisher 705/16
 2009/0177587 A1* 7/2009 Siegal et al. 705/67
 2009/0210347 A1* 8/2009 Sarcanin 705/67
 2009/0227281 A1* 9/2009 Hammad et al. 455/550.1
 2009/0266884 A1* 10/2009 Killian et al. 235/380
 2010/0057619 A1* 3/2010 Weller et al. 705/67
 2010/0063895 A1* 3/2010 Dominguez et al. 705/26
 2011/0212751 A1* 9/2011 Havens et al. 455/556.1
 2011/0320316 A1* 12/2011 Randazza et al. 705/26.43
 2012/0030044 A1* 2/2012 Hurst 705/18
 2013/0054470 A1* 2/2013 Campos et al. 705/67
 2013/0066742 A1* 3/2013 Stevens et al. 705/26.8
 2013/0173407 A1* 7/2013 Killian et al. 705/21

OTHER PUBLICATIONS

Hachman, M. (2002). Update: Sony, philips develop bluetooth-like tech ; sony and philips have agreed to jointly work on “near-field communication”, a potential competitor to bluetooth in the short-range personal area network (PAN) market. ExtremeTech.Com. , 1. Retrieved from <http://search.proquest.com/docview/213772240?accountid=14753>.
 Verifone: VeriFone announces QX120 contactless solution; versatile solution is EMV smartcard compliant and ready for mobile-phone initiated payments. (Nov. 12, 2007). M2 Presswire Retrieved from <http://search.proquest.com/docview/444611897?accountid=14753>.
 U.S. Appl. No. 11/933,337, Office Action mailed May 27, 2010, 9 p.
 U.S. Appl. No. 11/933,351, Office Action mailed Oct. 3, 2008, 5 p.
 U.S. Appl. No. 11/933,367, Office Action mailed May 27, 2010, 8 p.
 U.S. Appl. No. 11/467,441, Office Action mailed May 27, 2009, 17 p.
 U.S. Appl. No. 12/592,581, Office Action mailed Jun. 4, 2010, 20 p.
 U.S. Appl. No. 11/933,351, Office Action mailed Jul. 8, 2009, 7 p.
 U.S. Appl. No. 11/939,821, Office Action mailed Aug. 17, 2010, 11 p.
 U.S. Appl. No. 11/933,351, Office Action mailed Aug. 18, 2010, 16 p.
 U.S. Appl. No. 11/933,321, Office Action mailed May 27, 2010, 11 p.
 Deena, M. Amato, “Mobile Rewards.” Chain Store Age 82.5 (2006): 160, 161, 163. Hoover’s Company Profiles; ProQuest Central. Web. Oct. 5, 2012.
 “ViVOTech to Demonstrate Industry’s First End-to-End Near Field Communication (NFC) Solution at the NRF Show.” Business Wire: 1 Jan. 16, 2006. Business Dateline; Hoover’s Company Profiles; ProQuest Central. Web. Oct. 5, 2012.

* cited by examiner

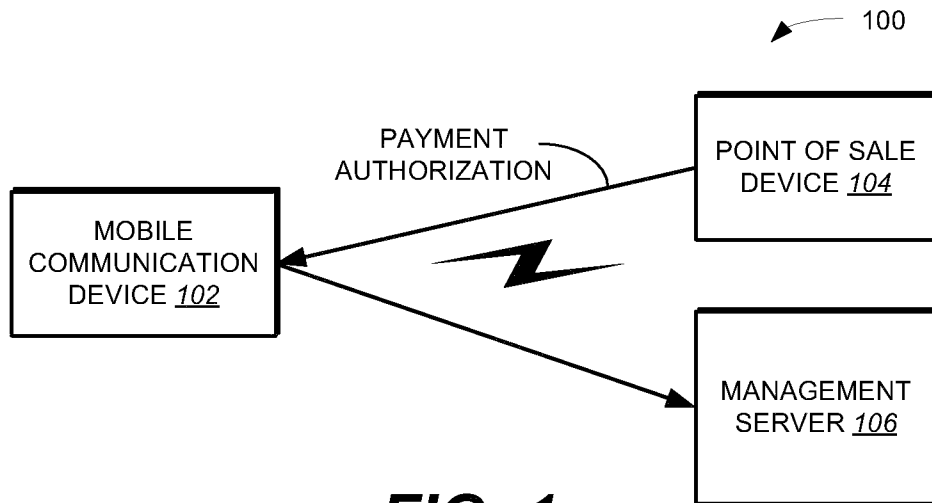


FIG. 1

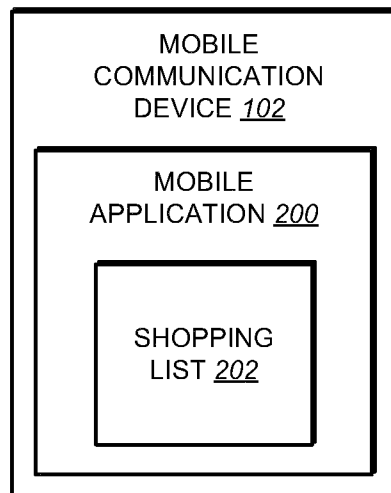


FIG. 2

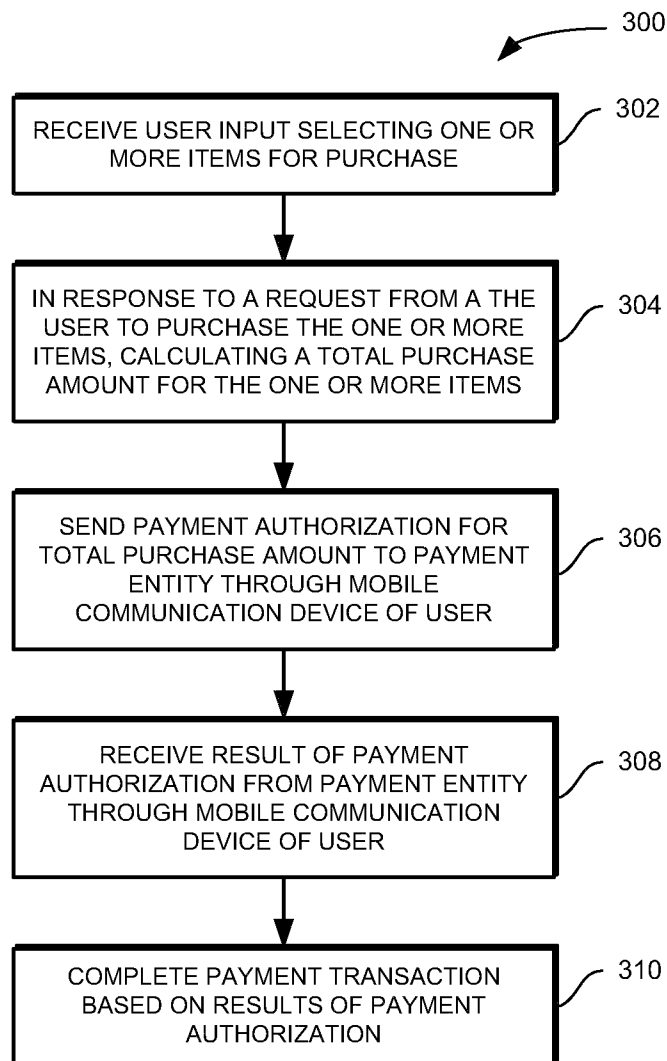


FIG. 3

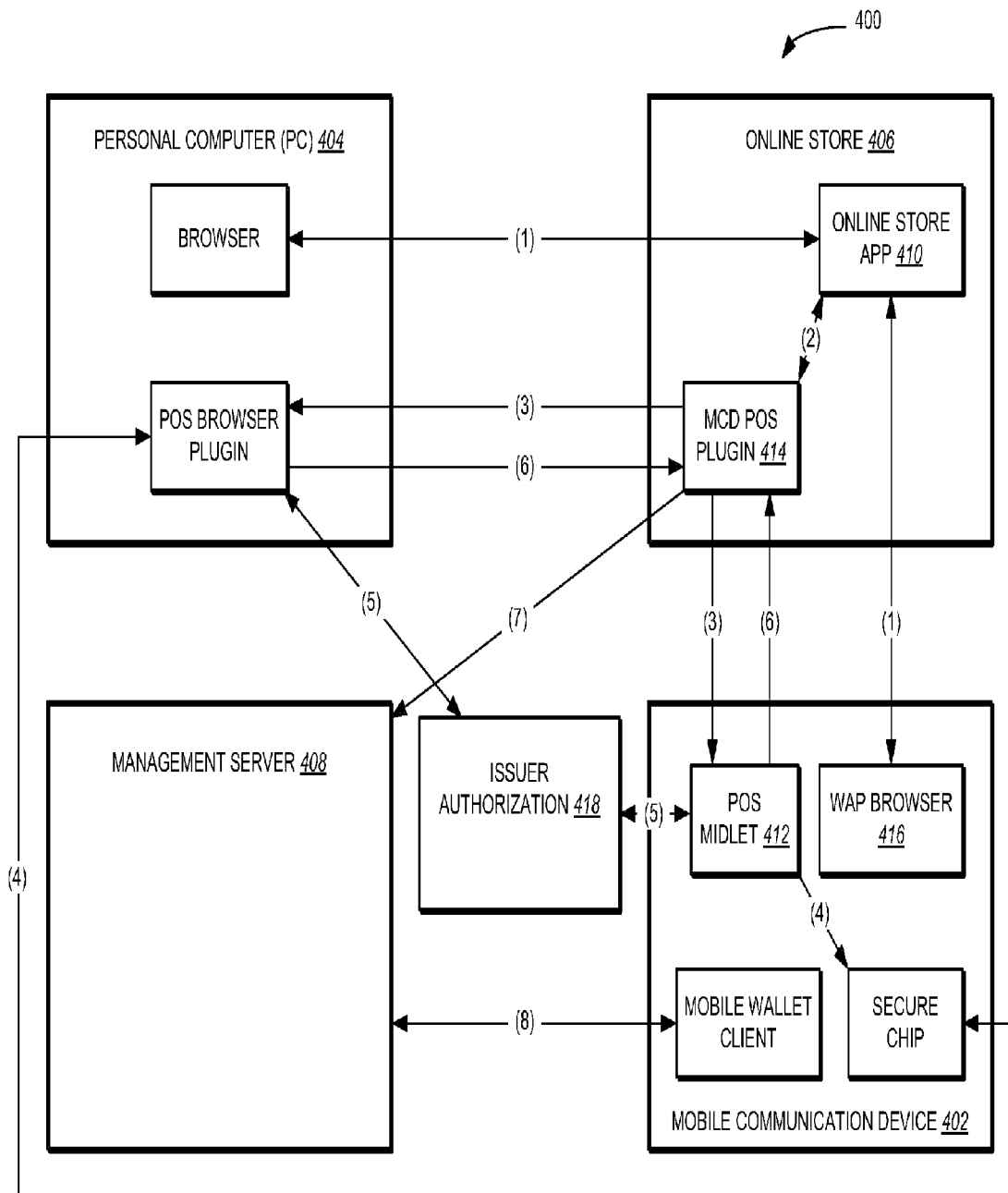


FIG. 4

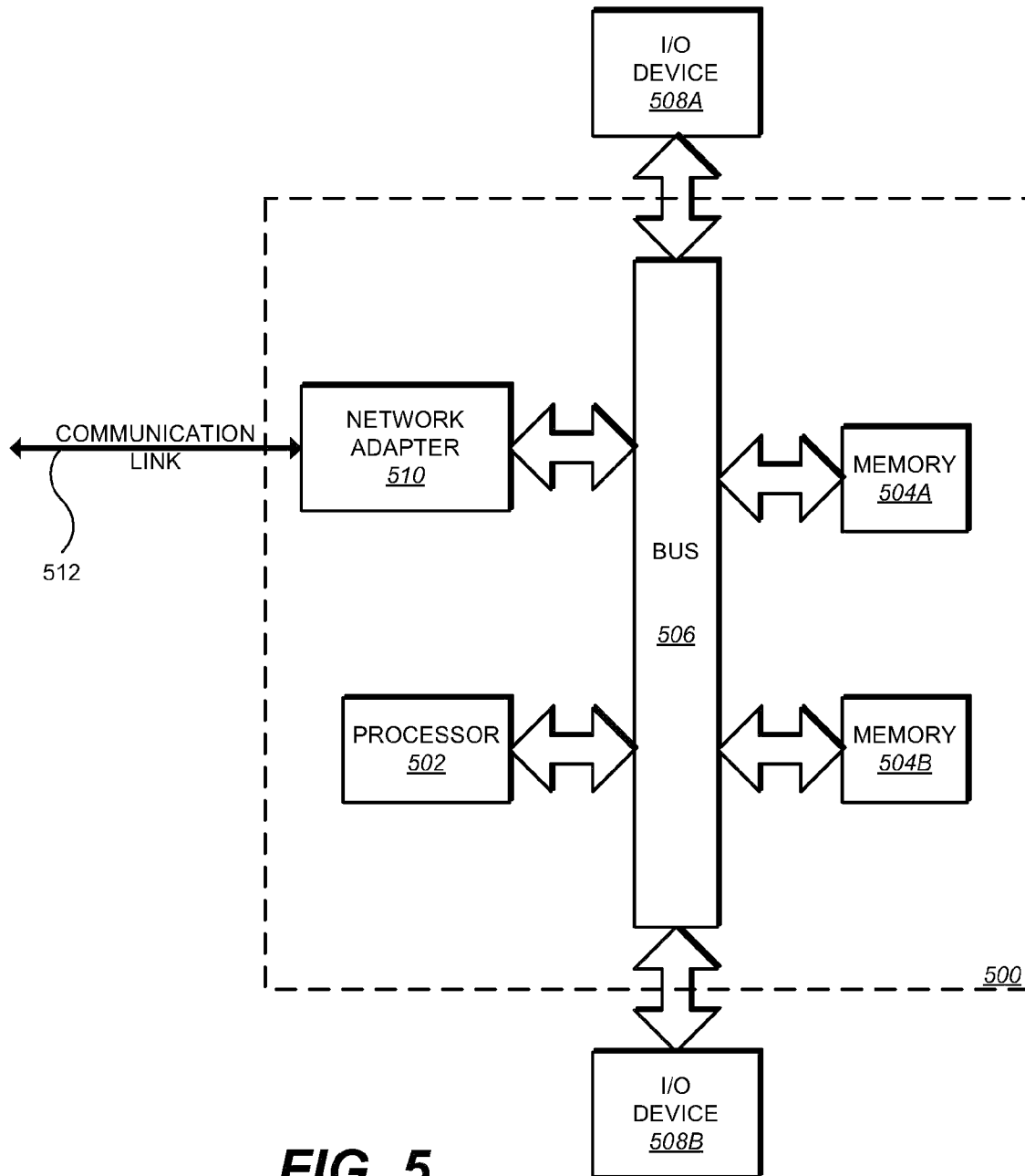


FIG. 5

1

UTILIZING A SECURE ELEMENT FOR NFC TRANSACTIONS WHICH INCLUDES RESPONSE DATA DURING INDUCTION

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of application Ser. No. 11/948,903, filed Nov. 30, 2007, titled METHOD AND SYSTEM FOR CONDUCTING AN ONLINE PAYMENT TRANSACTION USING A MOBILE COMMUNICATION DEVICE, all of which is incorporated by reference herein in its entirety.

FIELD OF INVENTION

The present invention relates to data communications and wireless devices.

BACKGROUND OF THE INVENTION

Mobile communication devices—e.g., cellular phones, personal digital assistants, and the like—are increasingly being used to conduct payment transactions as described in U.S. patent application Ser. No. 11/933,351, entitled “Method and System For Scheduling A Banking Transaction Through A Mobile Communication Device”, and U.S. patent application Ser. No. 11/467,441, entitled “Method and Apparatus For Completing A Transaction Using A Wireless Mobile Communication Channel and Another Communication Channel, both of which are incorporated herein by reference. Such payment transactions can include, for example, purchasing goods and/or services, bill payments, and transferring funds between bank accounts.

BRIEF SUMMARY OF THE INVENTION

In general, this specification describes a method and system for conducting an online payment transaction through a point of sale device. The method includes receiving input from a user selecting an item for purchase through the point of sale device; calculating a total purchase amount for the item in response to a request from the user to purchase the item; and sending payment authorization for the total purchase amount from the point of sale device to a payment entity, in which the payment authorization is sent to the payment entity via a mobile communication device of the user. The method further includes receiving a result of the payment authorization from the payment entity through the mobile communication device; and completing the payment transaction based on the result of the payment authorization.

Particular implementations can include one or more of the following features. The point of sale device can be a desktop computer, a laptop computer, or a terminal. The mobile communication device can be a cellular phone, a wireless personal digital assistant (PDA), or a laptop computer. The cellular phone can be an NFC-enabled phone. Sending payment authorization for the total purchase amount from the point of sale device to a payment entity can include sending the payment authorization securely to the payment entity. The payment entity can be a person, a computer system, or a bank. The method can further include maintaining a shopping list on the mobile communication device of the user, in which the shopping list includes a listing of one or more items to be purchased by the user. The payment authorization can be an authorization for payment with a credit card, a debit card, or a prepaid card.

2

The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features and advantages will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a block diagram of a communication system including a wireless mobile communication device and a management server in accordance with one implementation.

FIG. 2 illustrates one implementation of the wireless mobile communication device of FIG. 1.

FIG. 3 is a method for conducting a payment transaction using a point of sale device in accordance with one implementation.

FIG. 4 illustrates a block diagram of a communication system including a wireless mobile communication device and an online store in accordance with one implementation.

FIG. 5 is a block diagram of a data processing system suitable for storing and/or executing program code in accordance with one implementation.

Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates one implementation of a communication system **100**. The communication system **100** includes a handheld, wireless mobile communication device **102** a point-of-sale device **104** and a management server **106**. In one implementation, the mobile communication device **102** includes a mobile application (discussed in greater detail below) that permits a user of the mobile communication device **102** to conduct payment transactions. Payment transactions can include, for example, using contactless payment technology at a retail merchant point of sale (e.g., through point of sale device **104**), using mobile/internet commerce (e.g., purchase tickets and products, etc.), storage of payment information and other digital artifacts (e.g., receipts, tickets, coupons, etc.), storage of banking information (payment account numbers, security codes, PIN's, etc.), and accessing banking service (account balance, payment history, bill pay, fund transfer, etc.), and so on. The mobile communication device **102** can be a cellular phone, a wireless personal digital assistant (PDA), a laptop computer, or other wireless communication device. The point of sale device **104** can be a desktop computer, laptop computer, terminal, or other device that is configured to receive user input selecting items for purchase or other transaction.

In one implementation, authorizations for payment transactions that are made through the point of sale device **104** are sent from the point of sale device **104** to an issuer authorization (e.g., management server **106**) through the mobile communication device **102** (as shown in FIG. 1). In one implementation, an issuer authorization is a payment entity that either approves or disapproves a payment transaction. An issuer authorization can be, e.g., a person, computer system, bank (or other third party). One potential benefit of having payment authorizations flow through the mobile communication device **102** is that sensitive user information (e.g. account numbers, pin numbers, and/or identity information) need only be sent from the mobile communication device **102** directly to an issuer authorization. Such operation reduces the potential for identity theft and/or fraudulent purchases made through a point of sale device. For example, (in one imple-

mentation) payment authorizations cannot be sent to an issuer authorization if the mobile communication device **102** is turned off.

FIG. 2 illustrates one implementation of the mobile communication device **102**. The mobile communication device **102** includes a mobile application **200** that (in one implementation) is provided to the mobile communication device **102** through a remote server (e.g., management server **106**). In one implementation, the mobile application is a Mobile Wallet application available from Mobile Candy Dish, Inc., of Alameda, Calif. In one implementation, the mobile application is a hosted service, as described in U.S. patent application Ser. No. 11/939,821, entitled "Method and System For Securing Transactions Made Through a Mobile Communication Device", which is incorporated herein by reference. In one implementation, the mobile application **200** is configured to send requests to the management server for artifacts based on user input, e.g., received through a keypad (not shown) of the mobile communication device **102**. Requests to the management server **106** can also be automated, via proximity-based services, e.g., consumer tapping (or in close proximity) an LBS/contactless/RFID enabled phone against a smart poster (RFID/Bluetooth/LBS enabled, etc.), kiosk, or other device.

In one implementation, the mobile application **200** running on the mobile communication device **102** is configured to receive artifacts (e.g., advertisements, receipts, tickets, coupons, media, content, and so on) from the management server **106**. In one implementation, the management server **106** sends artifacts to the mobile application based on user profile information and/or a transaction history (or payment trends) associated with a user of the mobile communication device **102** as described in U.S. patent application Ser. No. 11/944,267, entitled "Method and System For Delivering Information To a Mobile Communication Device Based On Consumer Transactions", which is incorporated herein by reference.

In one implementation, the mobile communication device **102** is an NFC-enabled phone. The mobile communication device **102** can be NFC-enabled, for example, through an embedded chip or a sticker that is affixed to the cellular phone, as described in U.S. application Ser. No. 11/933,321, entitled "Method and System For Adapting a Wireless Mobile Communication Device For Wireless Transactions", which is incorporated herein by reference. In one implementation, the NFC chip (or sticker) on the cellular phone can be used in conjunction with a merchant's point of sale device as described in greater detail below.

For example, with reference to FIG. 4, in one implementation, the NFC chip (or sticker) on the cellular phone can communicate with NFC chips that are installed on the front of PC's (TV's, Kiosks, or any other device) and serve as scanners/readers. In this implementation a mobile candy dish applet (e.g., MCD POS plugin **414**) is installed on the consumer's computer (e.g., PC **404**) which interfaces with the NFC chip on the PC. When a consumer (or user) is shopping online and they are ready to pay for their products, the consumer opens his mobile wallet and selects one of the payment methods (e.g., credit card, debit card, prepaid card, etc.) from their mobile wallet. If a default card has been selected already, this step is not necessary. The consumer then waves their phone over the NFC reader present on the PC **404**. The consumer's payment credentials are transferred from the phone to the merchant website (e.g., online store application **410**) using a communication protocol between the chip in the phone and the chip in the PC, which can be radio frequency for example. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the

coupon, save the coupon for a future use (against a larger purchase for example), or have the coupon automatically applied during the transaction and the transaction amount is updated. After the consumer enters any necessary validation information (e.g., pin) to provide a multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant's online processor. The mobile wallet can retrieve transaction data, account balance from the management server **408**.

In one implementation, the mobile communication device **102** is a non NFC-enabled phone. In this implementation, the consumer connects his phone to the PC **404** via some non radio frequency method (e.g., IR, Bluetooth, USB cable, etc.). When a consumer is shopping online and they are ready to pay for their products, the consumer opens his mobile wallet and selects one of the payment methods (e.g., credit card, debit card, prepaid card, etc.) from their mobile wallet. If a default card has been selected already, this step is not necessary. The consumer then pushes, e.g., a "Buy now" button and the consumer's payment credentials are transferred from the phone to the merchant website (e.g., online store application **410**) using the protocol between the phone and the PC **404** which can be radio frequency, for example. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save the coupon for a future use, or have the coupon automatically applied during the transaction and the transaction amount is updated. After the consumer enters any necessary validation information (e.g., pin) to provide multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant's online processor. The mobile wallet can retrieve transaction data and account balance from the management server **408**.

In one implementation, the management server **408** and merchant portal (e.g., online store **408**) are maintained by trusted parties and use an encrypted tunnel to transfer financial data. When the consumer is ready to pay for their online product, they enter their cell phone number on the merchant portal. The merchant portal (which has an MCD applet (e.g., MCD POS plugin **414**) installed on its server) securely connects to the management server **408** (that in one implementation is maintained by Mobile Candy Dish (MCD)). In one implementation, the management server **408** identifies the consumer through their cell phone number, and verifies the consumer's authenticity by sending a unique transaction code to the consumer mobile wallet on their cell phone. The consumer then enters this unique transaction code onto the merchant's web portal. The merchant portal sends this transaction number to the management server **408** for authentication. Upon authentication, the consumer's virtual wallet and payment methods (e.g., credit card, debit card, prepaid card, etc.) are securely retrieved from the management server **408** and are displayed to the consumer in a window on a website associated with the merchant portal. The consumer selects one of these payment methods to pay for their transaction. If a default card has been selected already, this step is not necessary. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save the coupon for a future use, or have the coupon automatically applied during the transaction and the transaction amount is updated. After the consumer enters any necessary validation information to provide a multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant's online processor. The mobile wallet can retrieve transaction data, account balance from the management server **408**.

Referring to FIG. 2, in one implementation, the mobile application **200** maintains a shopping list **202** for a consumer. Accordingly, consumers have the ability to store their shopping list in their mobile wallet and add, delete, or change items on their shopping list either in offline or online mode. In one implementation, consumers are sent coupons based on items on their shopping list, preferences, previous shopping history, proximity to the physical retail store, or a combination of these parameters, as discussed in application Ser. No. 11/944,267, which is incorporated by reference above. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save the coupon for a future use, or have the coupon automatically applied during the transaction and the transaction amount is updated. When a consumer wants to order the items on their shopping list via an online merchant (in contrast to a physical retail store), the consumer can logon to the merchant portal and electronically transmit their shopping list to the merchant portal either by waving their phone over NFC enabled PC's or some other connection such as IR, bluetooth, USB, or the like.

FIG. 3 illustrates a method **300** for conducting a payment transaction using a point of sale device (e.g., point of sale device **104**). User input is received selecting one or more items for purchase (e.g., at the point of sale device) (step **302**). In general, the transaction being made at the point of sale device can be any type of transaction that involves the exchange or transfer of funds—e.g., the transaction can be a payment transaction, a fund transfer, or other type of transaction. In response to a request from the user to purchase the one or more items, a total purchase amount for the one or more items is calculated (e.g., by the point of sale device) (step **304**). If the user has coupons in their mobile wallet the user can either manually apply the coupon or have the coupon automatically applied during the transaction and the transaction amount is updated. The user request to purchase an item can be received, e.g., by a user clicking on a “buy now” icon that is displayed on a graphical user interface of the point of sale device. Payment authorization for the total purchase amount is sent to a payment entity through a mobile communication device of the user (step **306**). A result of the payment authorization is received at the point of sale device from the payment entity via the mobile communication device (step **308**). The payment transaction is completed based on the result of the payment authorization (step **310**). If the payment transaction was authorized by the payment entity, then the sale of the items through the point of sale device is completed. Otherwise, if the payment transaction was not authorized by the payment entity, then the point of sale device terminates the payment transaction.

FIG. 4 illustrates an example payment transaction being made in a communication system **400** in accordance with one implementation. The communication system **400** includes a mobile communication device **402**, a personal computer (PC) **404**, an online store **406**, and a core (or datastore) **408**. As indicated by interaction (1), a user (or customer), using a phone (e.g., mobile communication device **402** or personal computer **404**), browses an online store website (online store application **410**) and finds an item that the customer wishes to purchase. This could also be a purchase made through a midlet application (POS midlet **412**) residing on the mobile communication device **402**. The user then goes to, e.g., a checkout of the online store **406** make a purchase. If the user has coupons in their mobile wallet the user can either manually apply the coupon or have the coupon automatically applied during the transaction and the transaction amount is updated. When it comes time to authorize the purchase, (in one implementation) the user is given an option to purchase

with the mobile communication device **402**. In one implementation, the mobile communication device **402** is an NFC-equipped phone (or NFC phone).

In interaction (2), when the user chooses to purchase with the mobile communication device **402**, the online store application **410** sends the transaction information for authorization to the POS vendor plugin (e.g., MCD POS plugin **414**). In one implementation, the POS vendor plugin is installed in the merchant's online store and enables the merchant to accept MCD Blaze payments as an alternative form of payment, similar to accepting credit cards for payment. As shown by interaction (3), the POS vendor plugin formats, encrypts, and cryptographically signs the purchase authorization request which is sent via a secure SSL link (e.g., HTTPS, Bluetooth, IR, USB, or other suitable protocol) established by the browser/web application **416** back to the mobile communication device **402**. As with the first scenario, all communications is over secure channels. (It may be required that the mobile wallet application be opened prior to beginning a phone online purchase.) The POS midlet **412** is a component of the mobile wallet application that executes PayPass or other payment authorization protocol between itself and the SE payment applications on the mobile communication device **402** (interaction (4)). The results of the request are sent back to the POS vendor plugin.

As shown by interaction (5), the POS midlet **412** then forwards the properly formatted authorization request to a payment entity (e.g., issuer authorization **418**) for authorization. The results of the request are then sent back to the POS component of the mobile wallet. Through interaction (6), the POS midlet **412** then forwards the results back to the MCD POS plugin **414** to complete the purchase. The MCD POS plugin **414** then forwards the purchase transaction information to the management server **408** for later customer viewing (interaction (7)). As indicated by interaction (8), users (or customers) will then be able to query the management server **408** and immediately obtain purchase information, either by phone or PC.

One or more of method steps described above can be performed by one or more programmable processors executing a computer program to perform functions by operating on input data and generating output. Generally, the invention can take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment containing both hardware and software elements. In one implementation, the invention is implemented in software, which includes but is not limited to firmware, resident software, microcode, etc. Furthermore, the invention can take the form of a computer program product accessible from a computer-usable or computer-readable medium providing program code for use by or in connection with a computer or any instruction execution system. For the purposes of this description, a computer-usable or computer readable medium can be any apparatus that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or a propagation medium. Examples of a computer-readable medium include a semiconductor or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disk and an optical disk. Current examples of optical disks include compact disk—read only memory (CD-ROM), compact disk—read/write (CD-R/W) and DVD.

FIG. 5 illustrates a data processing system **500** suitable for storing and/or executing program code. Data processing sys-

tem **500** includes a processor **502** coupled to memory elements **504A-B** through a system bus **506**. In other implementations, data processing system **500** may include more than one processor and each processor may be coupled directly or indirectly to one or more memory elements through a system bus. Memory elements **504A-B** can include local memory employed during actual execution of the program code, bulk storage, and cache memories that provide temporary storage of at least some program code in order to reduce the number of times the code must be retrieved from bulk storage during execution. As shown, input/output or I/O devices **508A-B** (including, but not limited to, keyboards, displays, pointing devices, etc.) are coupled to data processing system **500**. I/O devices **508A-B** may be coupled to data processing system **500** directly or indirectly through intervening I/O controllers (not shown).

In one implementation, a network adapter **510** is coupled to data processing system **500** to enable data processing system **500** to become coupled to other data processing systems or remote printers or storage devices through communication link **512**. Communication link **512** can be a private or public network. Modems, cable modems, and Ethernet cards are just a few of the currently available types of network adapters.

Although the present invention has been particularly described with reference to implementations discussed above, various changes, modifications and substitutes are can be made. Accordingly, it will be appreciated that in numerous instances some features of the invention can be employed without a corresponding use of other features. Further, variations can be made in the number and arrangement of components illustrated in the figures discussed above.

What is claimed is:

1. A method comprising:
 - maintaining a secure element application in a secure element memory;
 - executing the secure element application maintained in the secure element memory using a secure element processor, the secure element memory and the secure element processor included in a secure element, wherein the secure element application configured for near field communication is executed in response to a near field communication trigger from a near field communication (NFC) terminal;
 - transmitting transaction data without prior authentication from the secure element to the NFC terminal which subsequently transfers the transaction data to a server for processing; and
 - receiving response information from the server via the NFC terminal at the secure element during the NFC interaction;
 - wherein the secure element is coupled to a mobile device comprising a mobile device processor, a mobile device memory that stores a non browser based mobile application, and a mobile device radio transceiver.
2. The method of claim 1, wherein the response information includes a coupon.
3. The method of claim 2, wherein the coupon is selected by the server and is based on user preferences, previous shopping history, and/or proximity to a store.
4. The method of claim 1, wherein the NFC terminal is a point-of-sale (POS) terminal.
5. The method of claim 1, further wherein the response information is transmitted from the secure element to a second secure element coupled to a second mobile device.

6. The method of claim 1, wherein the secure element is physically coupled to the mobile device and wirelessly coupled to electrical interior components of the mobile device.

7. The method of claim 1, wherein the secure element is included within the body of a memory card configured for placement in a memory card slot in the mobile device.

8. The method of claim 1, wherein the secure element is embedded within the body of the mobile device.

9. The method of claim 1, further wherein the mobile application is configured to allow items in a shopping list to be added, deleted, or changed.

10. A secure element comprising:

a secure element memory configured to maintain a secure element application;

a secure element processor that executes the secure element application configured for near field communication in response to a near field communication trigger from a near field communication (NFC) terminal, the secure element coupled to a mobile device comprising a mobile device processor, a mobile device memory that stores a non browser based mobile application, and a mobile device radio transceiver; and

a secure element transceiver that:

sends transaction data associated with a transaction without prior authentication from the secure element to the NFC terminal which subsequently transfers the transaction data to a server for processing; and

receives response information from the server via the NFC terminal during the NFC interaction.

11. The secure element of claim 10, wherein the response information includes a coupon.

12. The secure element of claim 11, wherein the coupon is selected by the server and based on user preferences, previous shopping history, and/or proximity to a store.

13. The secure element of claim 11, wherein the coupon is selected by the server and is based on spend category, merchant, and/or price level.

14. The secure element of claim 10, wherein the NFC terminal is a point-of-sale (POS) terminal.

15. The method of claim 1, wherein the secure element application is an identity application and the transaction data includes identity credentials.

16. The method of claim 1, wherein the secure element application is a ticket application and the transaction data includes payment credentials.

17. The method of claim 1, wherein the secure element application is a coupon application and the transaction data includes a coupon.

18. The secure element of claim 10, wherein the secure element application is a payment application and the transaction data includes payment credentials.

19. The secure element of claim 10, wherein the secure element application is an identity application and the transaction data includes identity credentials.

20. The secure element of claim 10, wherein the secure element application is a ticket application and the transaction data includes payment credentials.

21. The secure element of claim 10, wherein the secure element application is a coupon application and the transaction data includes a coupon.