US 20180225654A1

(19) **United States**

(12) **Patent Application Publication**

Mardikar et al.

(10) **Pub. No.: US 2018/0225654 A1**

(43) **Pub. Date: Aug. 9, 2018**

(54) **BIOMETRIC AUTHENTICATION OF MOBILE FINANCIAL TRANSACTIONS BY TRUSTED SERVICE MANAGERS**

(71) Applicant: **PAYPAL, INC.**, San Jose, CA (US)

(72) Inventors: **Upendra S. Mardikar**, San Jose, CA (US); **Eric Duprat**, San Jose, CA (US)

(21) Appl. No.: **15/859,260**

(22) Filed: **Dec. 29, 2017**

Related U.S. Application Data

(63) Continuation of application No. 14/529,692, filed on Oct. 31, 2014, now Pat. No. 9,858,566, which is a continuation of application No. 14/043,614, filed on Oct. 1, 2013, now abandoned, which is a continuation of application No. 13/418,196, filed on Mar. 12, 2012, now Pat. No. 8,554,689, which is a continuation of application No. 12/414,323, filed on Mar. 30, 2009, now Pat. No. 8,150,772.

(60) Provisional application No. 61/059,907, filed on Jun. 9, 2008, provisional application No. 61/059,395, filed on Jun. 6, 2008.

Publication Classification

(51) **Int. Cl.**

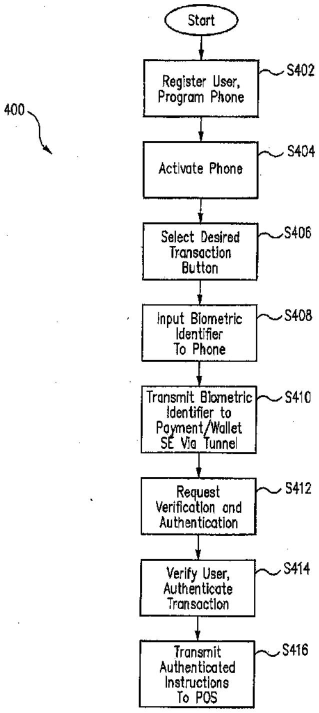
G06Q 20/32	(2012.01)
H04W 12/06	(2009.01)
G06Q 20/40	(2012.01)
G06Q 20/20	(2012.01)
H04L 29/06	(2006.01)
H04L 9/32	(2006.01)
G07F 7/08	(2006.01)
G07C 9/00	(2006.01)
G06Q 40/00	(2012.01)
G06Q 20/10	(2012.01)
G06Q 20/38	(2012.01)
G06Q 20/36	(2012.01)

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

CPC ***G06Q 20/3227*** (2013.01); *H04L 2209/80* (2013.01); ***G06Q 20/40*** (2013.01); ***G06Q 20/20*** (2013.01); ***H04L 63/0861*** (2013.01); ***H04L 63/0823*** (2013.01); ***H04L 9/3231*** (2013.01); ***G07F 7/0826*** (2013.01); ***G07C 9/00087*** (2013.01); ***G06Q 40/00*** (2013.01); ***G06Q 20/40145*** (2013.01); ***G06Q 20/4012*** (2013.01); ***G06Q 20/1085*** (2013.01); ***G06Q 20/3829*** (2013.01); ***G06Q 20/3821*** (2013.01); ***G06Q 20/382*** (2013.01); ***G06Q 20/3674*** (2013.01); ***G06Q 20/367*** (2013.01); ***G06Q 20/3278*** (2013.01); ***G06Q 20/3223*** (2013.01); ***G06Q 20/32*** (2013.01); ***G06Q 20/204*** (2013.01); *H04L 2209/56* (2013.01); ***H04W 12/06*** (2013.01)

(57) **ABSTRACT**

In one embodiment, a method comprises storing a biometric trait of a user in a data communication device of the user, comparing a biometric trait input into the device with the biometric trait stored in the device, generating a certificate authenticating the user within the device if the biometric trait input into the device matches the biometric trait stored in the device, and facilitating a financial transaction of the user using the certificate.


400
Start
Register User, Program Phone
S402
Activate Phone
S404
Select Desired Transaction Button
S406
Input Biometric Identifier To Phone
S408
Transmit Biometric Identifier to Payment/Wallet SE Via Tunnel
S410
Request Verification and Authentication
S412
Verify User, Authenticate Transaction
S414
Transmit Authenticated Instructions To POS
S416

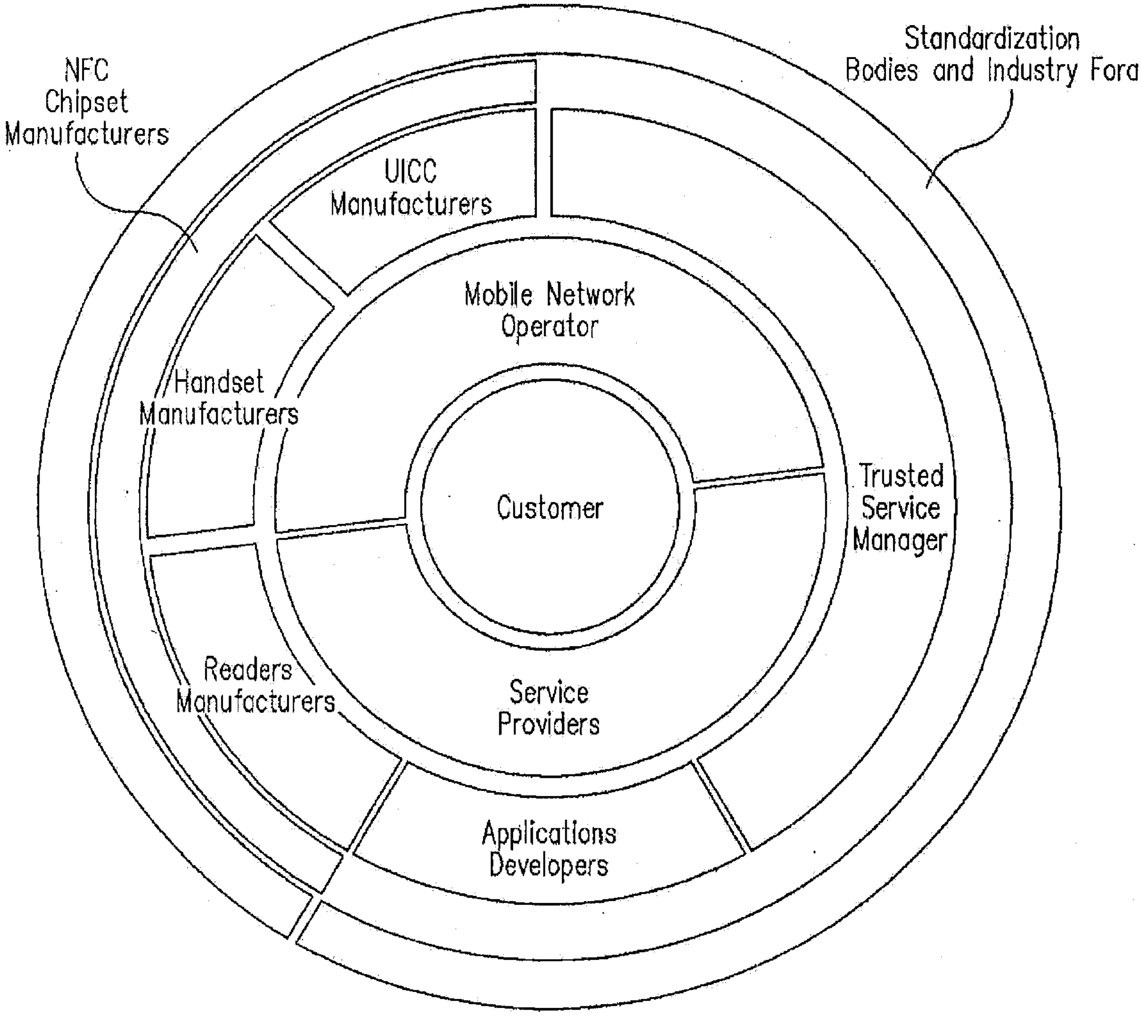

NFC
Chipset
Manufacturers
Standardization
Bodies and Industry Fora
UICC
Manufacturers
Mobile Network
Operator
Handset
Manufacturers
Customer
Trusted
Service
Manager
Readers
Manufacturers
Service
Providers
Applications
Developers

FIG. 1

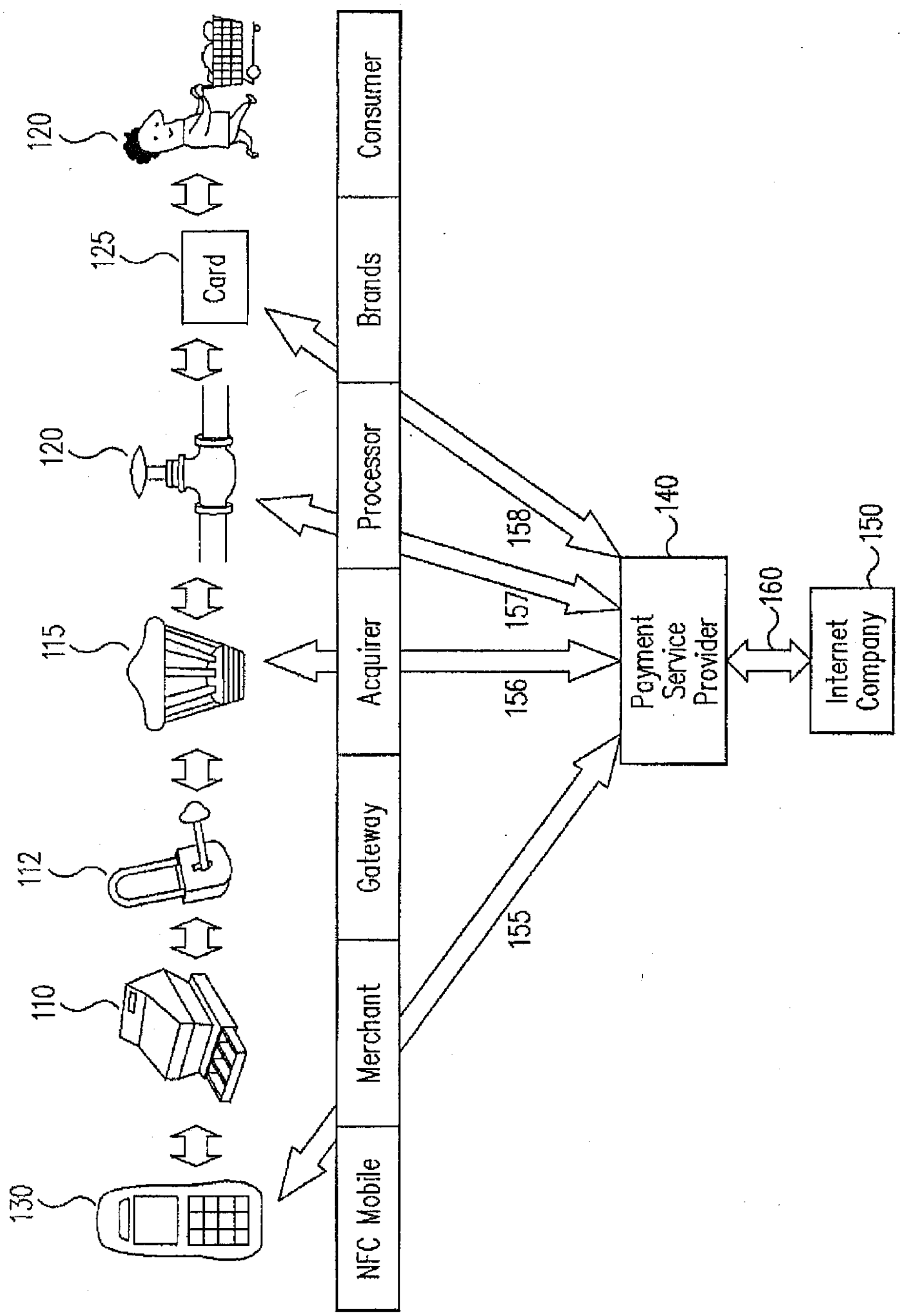

130
NFC Mobile
110
Merchant
112
Gateway
115
Acquirer
120
Processor
125
Card
Brands
120
Consumer
155
156
157
158
140
Payment Service Provider
160
150
Internet Company

FIG. 2

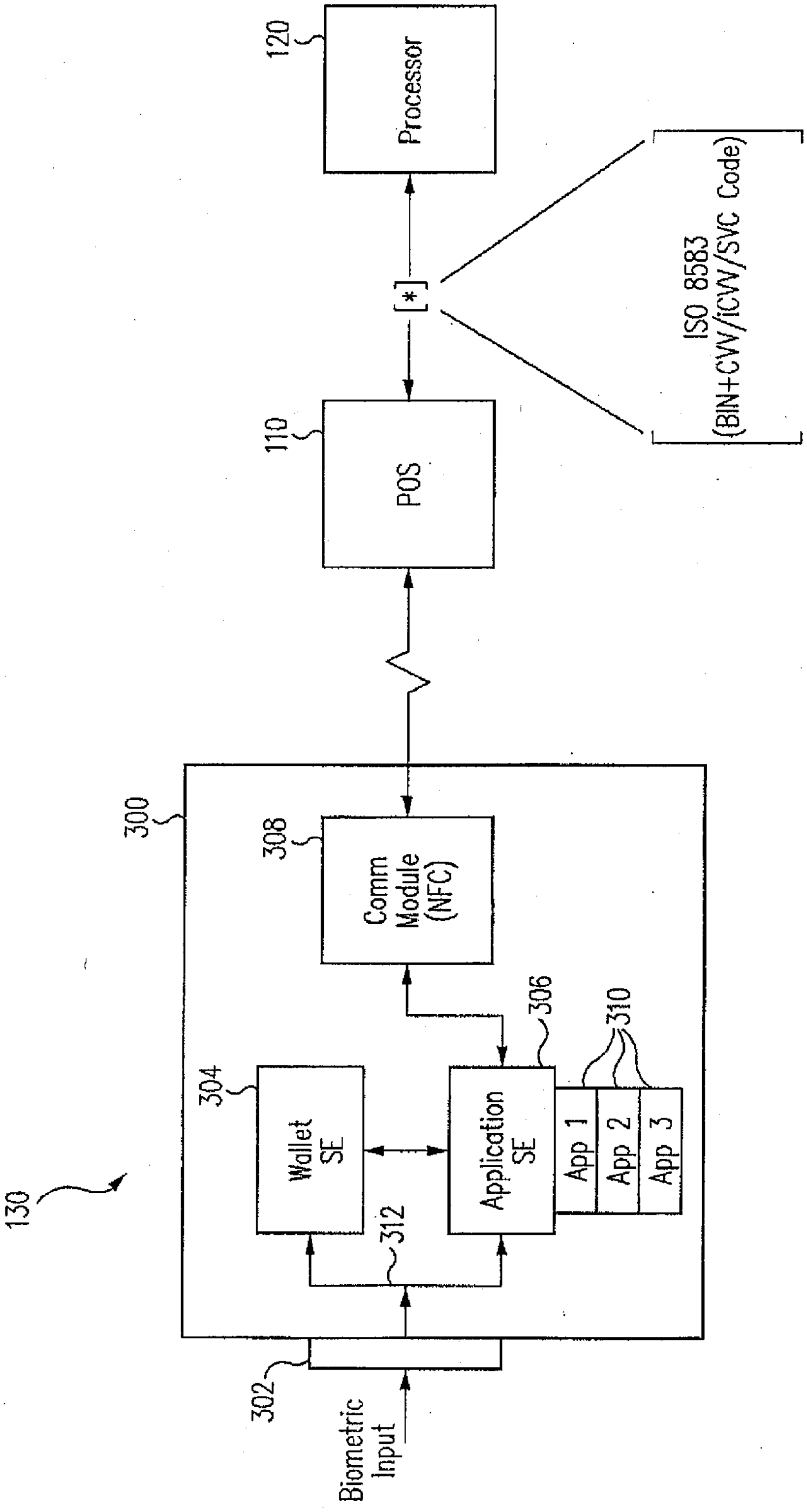

130
300
302
Biometric Input
312
304
Wallet SE
306
Application SE
310
App 1
App 2
App 3
308
Comm Module (NFC)
110
POS
[*]
ISO 8583
(BIN+CVV/iCVV/SVC Code)
120
Processor

FIG. 3

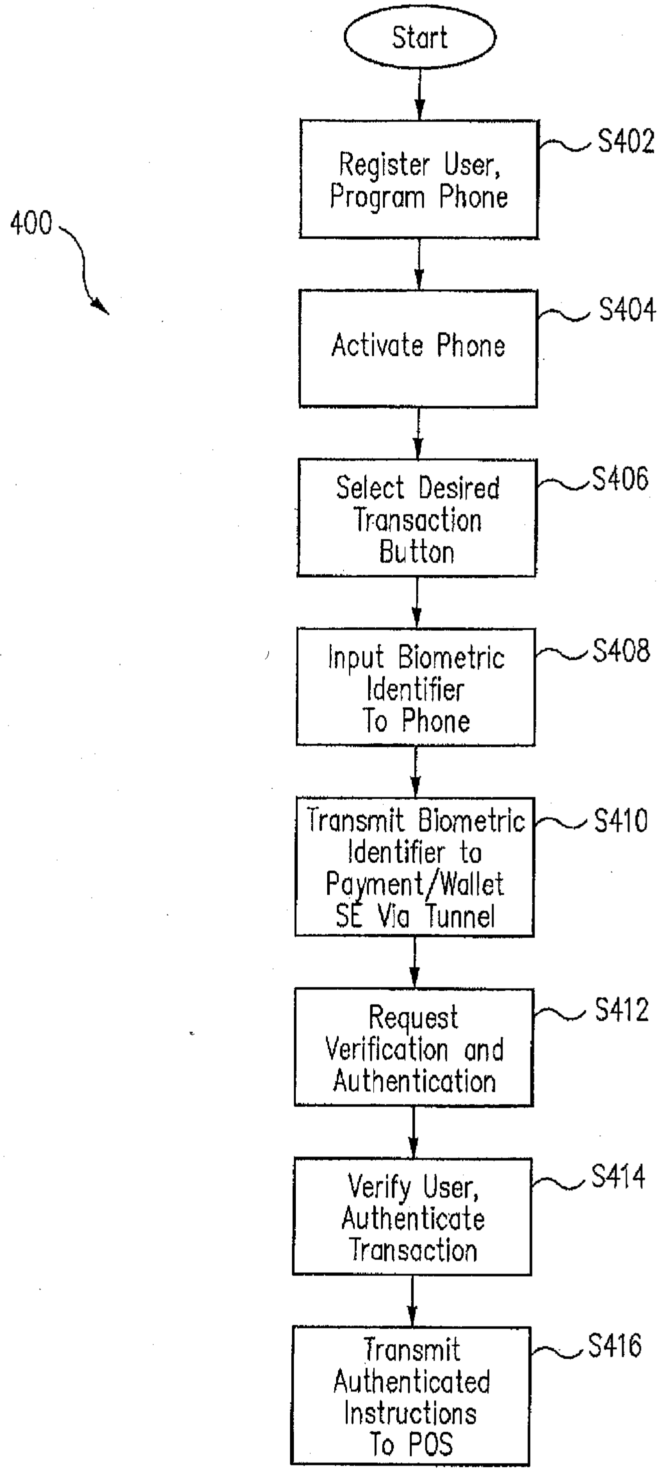

400
Start
Register User, Program Phone
S402
Activate Phone
S404
Select Desired Transaction Button
S406
Input Biometric Identifier To Phone
S408
Transmit Biometric Identifier to Payment/Wallet SE Via Tunnel
S410
Request Verification and Authentication
S412
Verify User, Authenticate Transaction
S414
Transmit Authenticated Instructions To POS
S416

FIG. 4

BIOMETRIC AUTHENTICATION OF MOBILE FINANCIAL TRANSACTIONS BY TRUSTED SERVICE MANAGERS

RELATED APPLICATIONS

[0001] This application is a continuation of U.S. patent application Ser. No. 14/529,692, filed Oct. 31, 2014, which is a continuation of U.S. patent application Ser. No. 14/043,614, filed Oct. 1, 2013, which in turn is a continuation of U.S. patent application Ser. No. 13/418,196, filed Mar. 12, 2012, now U.S. Pat. No. 8,554,689, which is a continuation of U.S. application Ser. No. 12/414,323, filed Mar. 30, 2009, now U.S. Pat. No. 8,150,772, and claims the benefit of U.S. Provisional Application Nos. 61/059,395, filed Jun. 6, 2008 and 61/059,907, Jun. 9, 2008, respectively, the entire disclosure of each of which are incorporated herein by reference.

BACKGROUND

1. Technical Field

[0002] This disclosure relates to electronic financial transactions in general, and more particularly, to methods and systems for biometric authentication of financial transactions by a trusted service manager (TSM).

2. Related Art

[0003] "Contactless technology" refers to short distance communications between two devices that are not physically connected. A wide variety of contactless technology exists today. Near Field Communication (NFC) is a specific type of contactless technology that is of high importance to Mobile Network Operators (MNOs) and to Service Providers (SPs), such as banks, credit card issuers and other payment service providers. NFC is a short-range, high frequency, wireless, RF communication technology that enables the exchange of data between devices typically over about a 10 centimeter (or about 4 inches) distance, thus providing a fast, simple and secure way for a user to effect a wide range of contactless services with a mobile device, such as a mobile telephone or personal digital assistant (PDA).

[0004] One example of an NFC technology application is financial transactions. NFC mobile devices and other types of contactless devices, such as radio frequency-enabled credit/debit cards, key fobs, and the like are experiencing rapid growth worldwide in various industries, including transportation, retail, parking and other industries, that will now accept NFC mobile payments and other types of contactless payments.

[0005] As an example, wireless mobile devices that include an NFC device and a smart card, which can use radio frequency identification (RFID) technology for identification purposes, can enable a person to effect a simple financial transaction, such as the purchase of a retail item, in a convenient, secure manner. Typically, a consumer waves the wireless mobile NFC device near a "reader" to effect a monetary transfer, and the purchase price of the item is deducted from a total amount that is available and stored on a "smart card" of the wireless mobile device. Optionally, the amount of the item can be forwarded to a server that can identify the purchaser through a unique identification code of the purchaser and then subsequently debit a credit or deposit account of the purchaser appropriately for the purchase of the retail item. Such NFC-based point of sale (POS) transactions provide several advantages, such as eliminating the need to carry cash and enabling faster, more convenient and secure financial transactions.

[0006] Because customers are interested in being able to use their mobile devices for contactless services, a new mobile NFC "ecosystem," illustrated in FIG. **1**, has been defined by the Global System for Mobile communication Association (GSMA), which is a global trade association representing over 700 GSM mobile phone operators throughout the world. (See, e.g., "Mobile NFC Services," GSMA, Version 1.0, February 2007). As illustrated in FIG. **1**, such ecosystems involve a variety of different players or entities and new roles for such players, including:

- **[0007]** Customer the customer is a customer of a merchant and subscribes to a Mobile Network Operator (MNO) and a service provider.
- **[0008]** MNO the MNO provides a full range of mobile services to the Customer, and can also provide Universal Integrated Circuit Cards (UICCs) and NFC terminals, plus Over the Air (OTA) transport mechanisms.
- **[0009]** Service Provider (SP) the SP provides contactless services to the Customer. Examples of SPs include banks, credit card issuers as well as public transport companies, loyalty programs owners, and the like.
- **[0010]** Retailer/Merchant the retailer/merchant can operate an NFC capable point of sale (POS) terminal.
- **[0011]** Trusted Service Manager (TSM) the TSM securely distributes and manages NFC applications and can have, for example, a direct or an indirect relation to the SPs, e.g., via clearing houses, such as the Automated Clearing House (ACH), the Electronic Payment Network (EPN) or the Visa/MasterCard network.
- **[0012]** Handset, NFC Chipset and UICC Manufacturers the Manufacturers produce mobile NFC/communication devices and the associated UICC hardware.
- **[0013]** Reader Manufacturer the reader manufacturer makes NFC reader devices.
- **[0014]** Application Developers the application developers design and develop mobile NFC applications, including financial transaction applications.
- **[0015]** Standardization bodies and industry associations develop global standards for NFC that enable interoperability, backward compatibility and future development of NFC applications and services.

[0016] As will be appreciated, successful implementation of NFC technologies requires cooperation between the many disparate players of the GSMA ecosystem. Each player can have its own expectations, for example, the Customer expects convenient, friendly and secure services within a trusted environment; the SPs want their applications to be housed and used in as many mobile devices as possible; and the MNOs want to provide new mobile contactless services that are secure, of high quality and consistent with the existing services experienced by the Customer. But although each player can have its own culture and expectations, they all have the same basic requirement, viz., the need for security and confidentiality.

[0017] The Trusted Service Manager (TSM), in particular, brings trust and convenience to the complex, multi-player NFC ecosystem. The TSM role includes providing a single point of contact for the SPs, e.g., banks, to access their respective customer bases through the MNOs, and to secure download and lifecycle management for mobile NFC applications on behalf of the SPs. It should be understood that the TSM does not disrupt the SP's business model, as the TSM does not participate directly in the transaction stage of the service, but rather, only indirectly.

[0018] In addition to NFC based POS payments, there are a number of other payment models currently prevalent in the mobile industry including:

[0019] (i) Short Message Service (SMS) SMS is a communications protocol that allows the interchange of short text messages between mobile devices; and,

[0020] (ii) Mobile Internet-based payments Customers routinely search for and purchase products and services through electronic communications with online merchants over electronic networks, such as the Internet.

[0021] Regarding the latter, individual customers may frequently engage in transactions with a variety of merchants through, for example, various merchant websites. Although a credit card can be used for making payments over the Internet, a disadvantage of online credit card usage is that online merchants can be exposed to high fraud costs and "chargeback fees" because there is no credit card authentication signature with an online sale.

[0022] In the case of in-person POS payments made with payment cards, such as with Master Cards or Visa cards in the U.S., or a "Chip and PIN" card in the U.K., current authentication is by means of the purchaser's provision of a signature or a personal identification number (PIN).

[0023] Accordingly, systems and methods are needed for authenticating NFC based POS transactions securely and reliably without the need for signatures or PINS, and more particularly, for authentication of POS transactions using a biometric trait, such as a fingerprint, that can be input via a data communication device of the user, e.g., the user's mobile phone.

SUMMARY

[0024] In accordance with the present disclosure, methods and apparatus are provided that enable the authentication of financial transactions to be indirectly effected as a value added service by a service provider acting as a TSM for credit/payment provider companies in which biometric authentication data of the transactions is provided directly at the POS via an NFC enabled mobile telephone without the need for the credit/payment providers having to provide it.

[0025] In one embodiment, a method comprises storing a biometric trait of a user in a data communication device of the user, comparing a biometric trait input into the device with the biometric trait stored in the device, generating a certificate authenticating the user within the device if the biometric trait input into the device matches the biometric trait stored in the device; and facilitating a financial transaction of the user using the certificate.

[0026] For example, in an embodiment at a point of sale (POS), a user could activate a mobile phone, invoke a application program stored in a first secure element (SE) therein, and then input a biometric trait to the phone, e.g., could swipe a thumb on a fingerprint reader of the phone. A second SE disposed within the phone might then verify the user's identity from the biometric trait input to the phone, and upon such verification, generate data sufficient to authenticate the transaction without having to contact and obtain authentication from, e.g., a third party credit/payment service provider. The data of the financial transaction, including the instruction codes therefor and the data authenticating the user, can then be transmitted from the phone to a data communication device of, for example, a merchant or vendor at the POS, which transmission, in one embodiment, can be effected via an NFC link between the phone and the POS device.

[0027] One or more of the storing of the application program in the first SE, the storing of the user's credentials in the second SE, and the generating of the data authenticating the transaction in response to the verification of the user's identity can comprise a value added service performed by a trusted service manager (TSM) on behalf of third party credit or a payment service providers.

[0028] A better understanding of the above and many other features and advantages of the novel TSM transaction authentication systems and methods of the present disclosure can be obtained from a consideration of the detailed description of some example embodiments thereof below, particularly if such consideration is made in conjunction with the several views of the appended drawings, wherein like elements are referred to by like reference numerals throughout.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] FIG. **1** is a schematic representation of a mobile NFC "ecosystem" defined by the Global System for Mobile communication Association (GSMA);

[0030] FIG. **2** is a schematic representation of the architecture of an example embodiment of an electronic payment system in accordance with the present disclosure;

[0031] FIG. **3** is a functional block and data flow diagram of an example embodiment of a mobile phone equipped with a POS transaction authenticating Secure Element (SE) architecture in accordance with the present disclosure engaged in transactional communication with a merchant's Point Of Sale (POS) device in accordance with the present disclosure; and,

[0032] FIG. **4** is flow diagram of an exemplary embodiment of a method for making a biometrically authenticated NFC based payment at a POS in accordance with the present disclosure.

DETAILED DESCRIPTION

[0033] In accordance with the embodiments described herein, methods and systems are provided that enable financial service providers, such as PayPal, acting in the role of a Trusted Service Manager (TSM), to authenticate NFC based POS transactions using biometric identifier traits, such as a fingerprint, that can be input via a data communication device of the user.

[0034] FIG. **2** is a schematic representation of an example embodiment of an electronic payment system in accordance with the present disclosure. A financial transaction using, for example, an NFC based Point of Sale (POS) payment system, can be made using a client data communication device **130**, such as an NFC enabled mobile phone, to a retailer or merchant via a retailer or merchant server **110**. It should be appreciated that although an NFC application is illustrated in this embodiment, the system is not limited to NFC applications, but can also apply to other types of applications, for example, video game consoles, DVRs, and other appliances.

[0035] The client device **130** can be implemented using any appropriate combination of hardware and/or software configured for wired and/or wireless communication over a network. For example, in one embodiment, the client device **130** can be implemented as a personal computer of a user **120** (also referred to herein as a "customer" or "consumer") in communication with the Internet or another network, such as a public switched telephone network (PSTN) and/or a private data network. In other embodiments, the client device **130** can be implemented as a wireless telephone, personal digital assistant (PDA), key fob, smart card, notebook computer or other type of data communication device. Furthermore, the client device **130** can be enabled for NFC, Bluetooth, online, infrared communications and/or other types of wireless data communication channels.

[0036] The client device **130** can include various applications as might be desired in particular embodiments to provide desired features to the client device **130**. Such applications could include, for example, security applications for implementing client-side security features, programmatic client applications for interfacing with appropriate application programming interfaces (APIs) over a network, or other types of applications.

[0037] The client device **130** can further include one or more user identifiers that could be implemented, for example, as operating system registry entries, cookies associated with a browser application, identifiers associated with hardware of client device **130**, or other appropriate identifiers. In one embodiment, a user identifier can be used by a payment service provider **140** to associate the client device **130** or the user **120** with a particular account maintained by a payment service provider **140**, such as PayPal, as described in more detail below.

[0038] Of importance, the client device **130** can further include a device useful for biometric authentication, such as a integral fingerprint scanner. Increasingly today, mobile phones are being equipped with such devices. When the phone is "flipped," or activated, the biometric trait reader reads the fingerprint of the user, confirms the identity of the user from the biometric trait, and upon confirmation of the user's identity, unlocks a credential/payment instrument located in one or more Secure Element(s) incorporated in the phone. As discussed in more detail below, when the phone is then "tapped" on an NFC enabled POS, an authenticated payment is effected via the user's biometric data input to the phone.

[0039] The merchant server **110** could be maintained, for example, by a retailer or by an online merchant offering various products and/or services in exchange for payment to be received over a network, such as the Internet. The merchant server **110** can be configured to accept payment information from the user **120** via, for example, the client device **130** and/or from a payment service provider **140** over a network. It should be appreciated that although a user-merchant transaction is illustrated in this particular embodiment, the system can also be applicable to user-user, merchant-merchant and/or merchant-user transactions.

[0040] The merchant server **110** can use a secure gateway **112** to connect to an acquirer **115**. Alternatively, the merchant server **110** can connect directly with the acquirer **115** or a processor **120**. Once verified, the acquirer **115**, which can also have a relation or subscription with the payment service provider **140**, processes the transaction through the processor **120** or the payment service provider **140**. "Brands" **125**, for example, bank payment card issuers, which also have a relation or subscription with the payment service provider **140**, are then also involved in the payment transaction so as to enable the user **120** to complete the purchase.

[0041] The payment service provider **140** can have data connections **155**, **156**, **157** and **158** with a subscriber client device **130**, a subscriber acquirer **115**, a subscriber processor **120** and/or a subscriber brand **125**, respectively, to communicate and exchange data. Such data connections **155**, **156**, **157** and **158** can take place, for example, via the Short Message Service (SMS) or a Wireless Application Protocol (WAP) over a network. In addition, according to one or more embodiments, the payment service provider **140** can have a data connection **160** with subscriber Internet companies, Internet mortgage companies, Internet brokers or other Internet companies **150**.

[0042] The payment service provider **140**, which can be an online payment provider, can provide payment on behalf of the user **120** to the operator of the merchant server **110** via the network **210**. In this regard, the payment service provider **140** includes one or more payment applications that can be configured to interact with the client device **130** and/or the merchant server **110** over the network **210** to facilitate the purchase of items by the user **120** from the merchant server **110**. In one embodiment, the payment service provider **140** can be provided by PayPal.

[0043] Each of the client data communication device **130**, the merchant server **110**, and the payment service provider **140** can include one or more processors, memories, and other appropriate components for executing instructions, such as program code and/or data stored on one or more computer readable mediums to implement the various applications, data, and methods described herein. For example, such instructions can be stored in one or more computer readable media, such as memories or data storage devices internal and/or external to various components of the system, and/or accessible over a network, which can be implemented as a single network or a combination of multiple networks, for example, the Internet or one or more intranets, landline networks, wireless networks, and/or other appropriate types of networks.

[0044] As discussed above, the payment service provider **140** can also serve in the role of a Trusted Service Manager (TSM). In one example embodiment of this, the payment service provider **140**, acting in the role TSM, can work cooperatively with a Mobile Network Operator (MNO) to incorporate an authentication certificate issued by the payment service provider, acting as a Certificate Authority (CA), in a Secure Element (SE) or Subscriber Identity Module (SIM) card **215** of a client device **130**. This SE or SIM card can follow security guidelines, such as The Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS 140-2 Level 2/3), a U.S. government computer security standard issued by the National Institute of Standards and Technology (NIST) and used to accredit cryptographic modules. The client device **130** can already have payment service provider issued certificates and user biometric trait information, such as the user's digitized fingerprint, stored within it for personalization purposes. When customers or users activate their payment service provider application **225**, such as a PayPal payment application, which can also be incorporated in the client device **130** in an "application SE," the users or customers are asked to select a PIN, which can be optional or mandatory. The PIN protects the private key of the authenticating certificate.

[0045] When a transaction, for example a financial transaction using NFC service application **217** of an NFC enabled client device **130**, is made via a payment service provider **140** such as PayPal, the service provider **140** receives signature information in the form of, for example, a X.509 certificate. X.509 is an ITU-T standard for a public key infrastructure (PKI) for single sign-on and Privilege Management Infrastructure (PMI). This X.509 signature information is typically maintained for each registered user of the service provider **140**. The signature information can be a digital signature and can include a time stamp, dollar amount, transaction type, item, and even location, which can be determined from a GPS enabled client device **130**. Signature information can also be preloaded in client device **130** in, for example, other applications, such as EMV (Europay, MasterCard, Visa), a standard for interoperation of IC cards ("Chip cards") and IC capable POS terminals and ATM's, for authenticating credit and debit card payments, or Elliptic Curve Cryptography (ECC), another form of public-key cryptography, in addition to X.509. In addition to NFC, the client device **130** can also be enabled for, e.g., Bluetooth, infrared or other types of communications and/or transactions.

[0046] FIG. **3** is a functional block and data flow diagram of an example embodiment of a client device **120** that comprises an NFC enabled mobile phone **300** engaged in transactional communication with a NFC enabled Point Of Sale (POS) data communication device **120** of, e.g., a merchant, in accordance with the present disclosure. In the particular embodiment of FIG. **3**, the phone **300** is equipped with a biometric trait data input device **302**, such as a fingerprint scanner, a POS transaction authenticating "Payment/Wallet" Secure Element (SE) **304**, an "Application" SE **306**, and an NFC communication module **308**, as described above.

[0047] With reference to FIG. **3**, it can be noted that the two SEs **304** and **306** comprise two separate elements, viz., a Payment/Wallet SE **304**, which can be, e.g., a SIM card, that stores only payment instruments, certificates, keys, user accounts, credentials and biometric trait authentication data, and the like, and an Application SE **306**, which can also be a SIM card, that stores only application programs **310** adapted to, e.g., generate instruction codes to effect final transactions, such as the purchase of goods or services or the transfer of money to or from the user. Thus, no user payment instruments, account data, certificates, keys or credentials reside in the Application SE **306**. In the particular embodiment illustrated, the Payment/Wallet SE **304** supports biometric trait authentication of the user, and the two SEs **304** and **306** are therefore split into two separate devices because, once the Payment/wallet SE **304** is certified by the TSM, such as through MasterCard or VISA, with the user's biometric trait data and other credential data, the phone **300** is then TSM-certified for use. Then, if it later becomes desirable to modify application programs of or add additional programs to the Application SE **306**, a new or re-certification procedure does not have to be performed each time they are modified or added, because applications do not need to be certified, whereas, Payment/Wallet SEs **306**, containing as they do the user's TSM-authenticated credentials, must be certified by the TSM before use with the affected payment service providers.

[0048] The initial set-up or programming of the Payment/Wallet SE **306** needs to be done only once, and can be performed at the premises of the TSM, or alternatively, over the air (OTA). Likewise, new or updated applications can be uploaded to the Applications SE **304** of the phone **300** either locally or OTA.

[0049] In one advantageous embodiment, the Payment/Wallet SE **306** can also be configured to store a list of transactions or account or receipt management information that can be viewed by the user at will on the phone **300** and/or downloaded to a PC for integration with the user's money management tools, such as Quicken, Microsoft Money, dedicated toolbars, or other PC software, such as expense management and expense submission tools and flexible spending account submissions.

[0050] As discussed above, current authentication of transactions via payment cards is typically by way of a user's signature or PIN. In Europe, authentication can also be via "Chip and PIN". However, as illustrated in FIG. **3**, in accordance with the present disclosure, the authentication of financial transactions, such as at a POS **110**, can be indirectly effected as a value added service by a service provider acting as a TSM for credit/payment provider companies, such as MasterCard and Visa, in which POS biometric authentication occurs directly via the mobile phone **300**. This biometric authentication can serve as signature/PIN/Chip and PIN/ARQC-ARPC authentication for all transactions. The authenticated transaction is then submitted to the POS device **110** via the NFC link between the NFC communication module **308** of the phone **300** and the POS device **110**. The POS device **110** receives the transaction as a pre-verified or pre-authenticated request, and in turn, transmits it to the host processor **120** for further processing in the form of an ISO 8583 message containing a Card Verification Value (CVV) code or a Contactless Card and Chip Verification (iCVV) code field, and other information, such as a Stored-Value Card (SVC) code and/or a bank identification number (BIN) code. Thus, a user's initial input of a biometric trait via the input device **302** can be used both to unlock the phone **300** and to authorize financial transactions without the need for the credit/payment providers having to do so.

[0051] FIG. **4** is flow diagram of an exemplary embodiment of a method **400** for making a biometrically authenticated NFC based payment at a POS **110** using the NFC and biometric trait data enabled phone **300** of FIG. **3** in accordance with the present disclosure. With reference to FIG. **4**, the method **400** begins at S**402** with the one-time setup or user registration procedure with the TSM as described above.

[0052] After the initial registration of the user with the TSM is complete, during which step S**402**, the Payment/Wallet SE **304** of the phone **330** is programmed with the user's credentials and the Application SE **306** of the phone **300** is programmed with one or more suitable financial transaction application programs **310**, the phone **300** is then ready for use in making authenticated financial transactions. In an example purchase transaction at a POS **110**, such as illustrated in FIG. **3**, the user, in the role of a purchaser, can, at S**404**, first activate the phone **300**, e.g., by opening it. At S**406**, the user can then select a "Make Payment" button on the phone **300**. Selecting the Make Payment button invokes a suitable payment application program **310** in the Application SE **306** of the phone **300** that is adapted to, among other things, read a biometric trait of the user, e.g., the user's thumb-print and request verification of it by the Payment/Wallet SE **304**.

[0053] At S**408**, the user-purchaser then swipes his or her thumb on the biometric trait input device **302** of the phone **302**, and at S**410**, this biometric trait input is fed directly to the Payment/Wallet SE **304** of the phone **300** via a "tunnel" circuitry **312**. Optionally, the thumb swipe can also be operable to unlock the phone for use. Preferably, a tunnel circuit **312** is used for security purposes because the architecture of the user's fingerprint is such that it can otherwise be captured by an application on a mobile phone. To prevent this, a tunnel encryption circuitry **312** that is FIPS 140-2 level 3 compliant is incorporated in the phone **300** so that the fingerprint data goes directly to the Payment/Wallet SE **304** of the phone **300** for authentication and unlocking.

[0054] At S**412**, the payment application **310** that was invoked by pressing the Make Payment button sends a message to the Payment/Wallet SE **304** requesting user verification and payment authentication. At S**414**, when the Payment/Wallet SE **304** verifies the user's thumbprint, and based thereon, authenticates the payment, the Payment/Wallet SE **304** sends the authenticated payment (or other) instructions back to the payment application **310**, which then sends it to the NFC communication module **308** of the phone **300**.

[0055] At S**416**, when the user then "taps" the phone **300** on the merchant's POS device **110**, the pre-authenticated payment instructions are transmitted via an NFC link to the POS device **110**, and thence, to the merchant's processor device **110**. As above, the payment instructions include not only all of the payment information needed to effect the transaction, such as the user's account information or credit balance, but also all of the information necessary to authenticate the transaction, including CVV, iCVV, SVC and/or BIN codes, without the need for the credit/payment service providers having to provide it.

[0056] As those of skill in this art will appreciate, although the foregoing method is described in the context of a transaction involving a purchase of goods or services at a POS, it is evident that it can be made applicable to other types of financial transactions, such as the deposit or withdrawal of cash at an automated teller machine (ATM).

[0057] Although various components and steps have been described herein as being associated with the client device **130**, merchant server **110**, and payment service provider **140** of FIGS. **1-3**, it is contemplated that the various aspects of such servers illustrated in FIGS. **1-3** can be distributed among a plurality of servers, devices, and/or other entities. For example, in one embodiment, transaction record processing application **290** and transaction records **295** can be implemented by an entity separate from payment service provider **140**. Accordingly, in such an embodiment, communications described herein performed in relation to transaction record processing application **290** and transaction records **295** can be provided to a separate entity and need not be routed through payment service provider **140** in all instances.

[0058] Where applicable, various embodiments provided by the present disclosure can be implemented using hardware, software, or combinations of hardware and software. Also where applicable, the various hardware components and/or software components set forth herein can be combined into composite components comprising software, hardware, and/or both without departing from the spirit of the present disclosure. Where applicable, the various hardware components and/or software components set forth herein can be separated into sub-components comprising software, hardware, or both without departing from the spirit of the present disclosure. In addition, where applicable, it is contemplated that software components can be implemented as hardware components, and vice-versa.

[0059] Software in accordance with the present disclosure, such as program code and/or data, can be stored on one or more computer readable media. It is also contemplated that software identified herein can be implemented using one or more general purpose or specific purpose computers and/or computer systems, networked and/or otherwise. Where applicable, the ordering of various steps described herein can be changed, combined into composite steps, and/or separated into sub-steps to provide the features described herein.

[0060] The foregoing disclosure is not intended to limit the present disclosure to the precise forms or particular fields of use disclosed. It is contemplated that various alternate embodiments and/or modifications to the present disclosure, whether explicitly described or implied herein, are possible in light of the disclosure.

[0061] Although the apparatus and methods of the present invention have been described and illustrated herein with reference to certain specific example embodiments thereof, it should be understood that a wide variety of modifications and variations can be made to these without departing from the spirit and scope of the invention, as defined by the claims appended hereafter and their functional equivalents.

1. An application function authorization system, comprising:

a first secure element that is located in a user device and that is configured to provide a first application;

a second secure element that is located in the user device, that is coupled to the first secure element, and that stores user authentication data and application function authorization information; and

tunnel circuitry that is coupled to the second secure element and that is configured to prevent access to user data transmitted through the tunnel circuitry by non-authorized subsystems in the user device, wherein the second secure element is configured to:

receive user data transmitted through the tunnel circuitry;

verify the user data using the user authentication data; and

provide, in response to the verification of the user data, the application function authentication information to the first application provided by the first secure element in order to enable the application to perform an application function.

2. The system of claim **1**, wherein the application function includes generating transaction instructions for processing a transaction.

3. The system of claim **1**, wherein the first secure element is configured to provide at least one second application.

4. The system of claim **1**, further comprising:

a user data input device coupled to the tunnel circuitry and configured to receive the user data from a user.

5. The system of claim **4**, wherein the user data input device is a user biometric trait input device that is configured to receive user biometric trait data from the user.

6. The system of claim **1**, wherein the first secure element is a Trusted Service Manager (TSM) certified by a third party.

7. The system of claim **1**, wherein the application function includes a wireless transmission.

8. A method for authorizing an application function, comprising:

transmitting, via tunnel circuitry to a first secure portion of a secured system, user data, wherein the tunnel circuitry prevents access to transmitted user data by non-authorized subsystems;

authenticating, using the first secure portion of the secured system via user authentication data that is stored in the secure portion of the secured system, the user data; and

transmitting, from the first secure portion of the secured system to a first application provided by a second secure portion of the secured system in response to authenticating the user data, application function authorization information that is stored in the first secure portion of the secured system, wherein the application function authorization information enables the first application to perform an application function.

9. The method of claim **8**, wherein the application function includes generating payment instructions for completing a payment.

10. The method of claim **9**, further comprising:

providing, using the second secure portion of the secured system, at least a second application.

11. The method of claim **8**, further comprising:

receiving, from a user data input device coupled to the tunnel circuitry, the user data from a user.

12. The method of claim **11**, wherein the user data input device is a user biometric trait input device that receives user biometric trait data from the user.

13. The method of claim **8**, wherein the second secure portion of the secured system is a Trusted Service Manager (TSM) certified by a third party.

14. The method of claim **8**, wherein the application function includes a wireless transmission.

15. A non-transitory machine-readable medium having stored thereon machine-readable instructions executed to cause a machine to perform operations comprising:

transmitting, through tunnel circuitry located in a device, user data to a first security module, wherein access to the user data by non-authorized subsystems in the device is prevented by the tunnel circuitry;

accessing user authentication data and application function authorization information from the first security module;

determining, through the first security module, whether the user data matches the user authentication data; and

releasing, through the first security module, the application function authorization information to a first application that is provided by a second security module that is located in the device in response to determining a match between the user data and the user authentication data, wherein the authentication function authentication information enables the application to perform an application function.

16. The non-transitory computer readable medium of claim **15**, wherein the application function includes generating instructions for transferring money.

17. The non-transitory computer readable medium of claim **16**, wherein the operations further comprise:

providing, through the second security module, at least one second application.

18. The non-transitory computer readable medium of claim **15**, wherein the operations further comprise:

receiving, through a user data input device located in the device and coupled to the tunnel circuitry, the user data from a user.

19. The non-transitory computer readable medium of claim **18**, wherein the user data input device is a user biometric trait input device that receives a user biometric trait data from a user.

20. The non-transitory computer readable medium of claim **15**, wherein the second security module is a Trusted Service Manager (TSM) certified by a third party.

* * * * *