

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
13 December 2007 (13.12.2007)

PCT

(10) International Publication Number  
**WO 2007/143740 A2**

(51) International Patent Classification:

G06Q 30/00 (2006.01)

(21) International Application Number:

PCT/US2007/070679

(22) International Filing Date: 8 June 2007 (08.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/811,982 8 June 2006 (08.06.2006) US

(71) Applicant (for all designated States except US): **MAS-TERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **FORAN-OWENS, Elizabeth, M.** [US/US]; 44 Davenport Drve, Stamford, CT 06902 (US). **WANKMUELLER, John** [US/US]; 35 Tan-ners Road, Great Neck, NY 10020 (US). **RADU, Cristian** [BE/BE]; Rue De Tourinnes 2, B-1320 Beauvechain (BE).

(74) Agents: **SCHEINFELD, Robert, C.** et al.; Baker Botts L.L.p., 30 Rockefeller Plaza, New York, NY 10112-4498 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

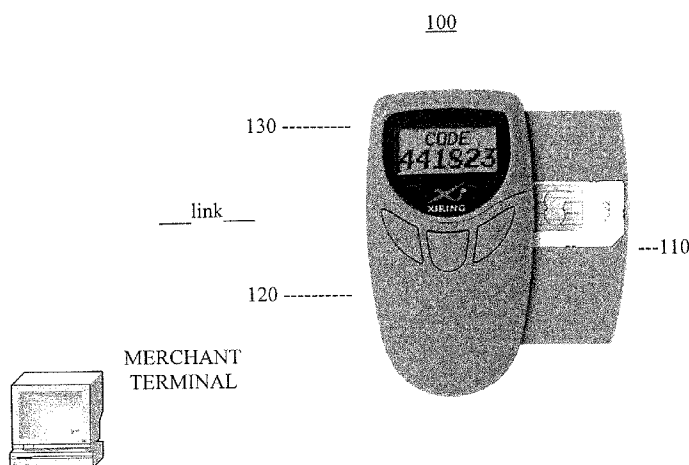
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ALL-IN-ONE PROXIMITY PAYMENT DEVICE WITH LOCAL AUTHENTICATION



All-In-One Xiring device (with on/off feature and CAP feature) having PayPass functionality. The device has a PIN CVR "indicator" to merchant POS components. The device provides a new PIN management feature and re-uses current message infrastructure where the merchant terminal receives a transaction that has already been approved (signed) by the consumer.

(57) Abstract: A personal powered proximity payment device that can be owned by or issued to an individual user is provided. The device is a non-ISO card device that includes an internal dual-mode (contact and contactless) chip card coupled to a display and a robust PIN entry or biometric reading means. The device provides proximity payment functions, and optional proximity payment on/off and local pre- purchase account holder verification functions to the individual user.

WO 2007/143740 A2

## **ALL-IN-ONE PROXIMITY PAYMENT DEVICE WITH LOCAL AUTHENTICATION**

### CROSS-REFERENCE TO RELATED APPLICATIONS

5           This application claims priority to U.S. Provisional Application Serial No. 60/811,982, filed June 8, 2006, which is incorporated by reference herein in its entirety.

### BACKGROUND OF THE INVENTION

Smart card technology is fast becoming commonplace in our culture and  
10   daily lives. A smart card is a card that is embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. The microprocessor card can add, delete, and otherwise manipulate information on the card, while a memory-chip card (for example, pre-paid phone cards) can only undertake a pre-defined operation. Smart cards, unlike magnetic stripe cards, can  
15   carry all necessary functions and information on the card. Therefore, they do not require access to remote databases at the time of the transaction.

Smart cards, which are also generally referred to by the industry as “microprocessor cards” or “chip cards”, offer greater memory storage and security of data than traditional magnetic stripe cards. Smart cards may have up to 8 kilobytes of  
20   RAM, 346 kilobytes of ROM, 256 kilobytes of programmable ROM, and a 16-bit microprocessor. A smart card uses a serial interface and receives its power from external sources like a card reader. The processor uses a limited instruction set for applications such as cryptography. Smart cards are used for a variety of applications, especially those that have cryptography built in, which require manipulation of large

numbers. Thus, smart cards have been the main platform for cards that hold a secure digital identity. The most common smart card applications are:

- \* Credit cards
- \* Electronic cash
- 5       \* Computer security systems
- \* Wireless communication
- \* Loyalty systems (like frequent flyer points)
- \* Banking
- \* Satellite TV
- 10       \* Government identification

Delivering security – i.e., ensuring access is granted only for authorized usage by authorized cardholders – is the fundamental attribute of smart cards. The effectiveness of smart cards in delivering security is one of the reasons they have been so widely adopted, especially in financial services and mobile phones, why the growth

15 of smart cards has been explosive, and why their usage is expected to expand rapidly for other applications such as personal identity cards, access to pay TV/entertainment, health care services and transportation. Assignee MasterCard makes smart card based authentication solutions (e.g., a program called the Chip Authentication Program (CAP)) available to card issuers. CAP can also be used for Internet banking and other

20 applications requiring positive cardholder authorization. (See, e.g., Rutherford et al., International Patent Publication No. WO/2005/001618, Wankmueller et al., International Patent Publication No. WO/2003/081832, and. Harris et al., International Patent Publication No WO/2001/027887, all of which publications are incorporated by reference herein).

For contactless payment card systems to be economically viable and to gain commercial acceptance, the contactless payment cards must be interoperable at all or most RFID-enabled payment terminals, even when the cards and terminals have technological features that are proprietary to specific card providers/issuers, vendors or terminal manufacturers. Industry-wide interoperability is desirable. Towards this end, industry standards organizations and groups (e.g., International Organization for Standards (ISO) and International Electro Technical Committee (IEC)) have formulated voluntary industry standards for implementation of contactless smart card payment technologies. Three such exemplary standards which have been defined by ISO/IEC are the ISO/IEC 10536, ISO/IEC 14443, and ISO/IEC 15693 standards applicable to Close Coupling, Proximity and Vicinity cards, respectively.

Recently, assignee MasterCard International Incorporated ("MasterCard") has developed proprietary specifications MasterCard PayPass™ ISO/IEC 14443 Implementation Specification ("PayPass") for implementation of proximity (contactless) payment card technologies. PayPass is an RF-enabled contactless payment platform, which lets users tap or wave a device in front of a special reader in order to process a transaction. The PayPass implementations are consistent with the ISO/IEC 14443 Standard and provide a convenient example illustrating the principles of the present invention. See, e.g., Smets et al., U.S. patent application Nos. 11/182,354, 11/182,357, 11/182,358, 11/182,356, 11/182,355, and 11/182,351, all filed July 15, 2005 and all of which are incorporated by reference herein.

In addition to contactless technologies that are standardized under ISO 14443, a number of proprietary contactless interfaces are also used in the industry (e.g., Cubic's GO-Card and Sony's FeliCa card). With existing card technology deployments, interoperability can be an issue. Card readers deployed by vendors in

the marketplace should preferably accommodate several different card types. For example, a desirable card reader would support ISO 14443 cards, any additional proprietary card types and also existing “contact” payment cards. A method and system for conducting transactions using a payment card with two different technologies is described in Wankmueller U.S. Patent No. 6,857,566, which is incorporated by reference herein in its entirety.

Consideration is now being given to enhancing electronic payment solutions and devices. Attention is being directed to non-standard electronic payment devices with a view to integrating the features of both contact and non-contact payment devices.

Further features of the invention, its nature and various advantages will be more apparent from the accompanying drawings and the following detailed description.

#### SUMMARY OF THE INVENTION

Proximity payment devices and methods with local authentication features for facilitating proximity payment transactions are provided.

An exemplary proximity payment device (“all-in-one” proximity payment device) includes an internal dual-mode (contact and contactless) chip card. The all-in-one device further includes an ISO 14443 antenna connected to the chip card for contactless operation. Further, the dual-mode chip card includes proximity payment applications (such as MasterCard’s PayPass application) for contactless operation. The contact portions of the chip have integrated PIN entry and/or biometric reader capability (e.g., via chip contact plates). The chip is configured to provide local verification of the PIN or biometric signature submitted by a user. The dual-mode

chip card includes contact chip applications (e.g., MasterCard's CAP user authentication application) for this purpose and other purposes.

The local verification feature of the all-in-one device advantageously eliminates the need to have the proximity device/account holder (e.g., a PayPass payment account holder) enter his or her PayPass payment account PIN or biometric signature into a separate merchant device for making a proximity payment transaction. The feature also advantageously dispenses with the need to have a separate PIN entry device at the merchant point of interaction. Instead, the PIN or biometric signature can be submitted or entered in the account holder's own device.

10 The all-in-one device allows PayPass transactions of any dollar size to be transacted without requiring merchants to deploy any user transaction verification hardware (e.g., PIN Pads or biometric readers).

In a method for making a customer-merchant transaction using the all-in-one device, the merchant terminal (or POS device, ATM etc.) receives a transaction that has already been approved or signed by the consumer. Thus, the merchant POS device does not have to prompt the customer for PIN or a biometric signature entry. In one embodiment, the all-in-one device generates a chip produced Cardholder Verification Result (PIN-Flag), which is sent to the all-in-one device issuer and is of use only for the upcoming payment transaction.

20 In an embodiment of the invention, the all-in-one device is a battery-powered PayPass device having a display and PIN entry or biometric reading capability. The device is a "non-ISO card" device that uses an internal dual-mode (contact and contactless) chip card. The battery-powered PayPass device has the usual PayPass functions and may further have an optional PayPass on/off switching

25 function and an optional PayPass pre-purchase account holder verification function.

The beneficial features of this all-in-one device include: a) the use of the display, and b) PIN entry or biometric reader capability of the device for a number of optional controls of the PayPass payment application.

In the operation of this all-in-one device, a user can activate the PayPass on/off function (e.g., by manually depressing a “power on” switch or pushbutton) to enable proximity PayPass chip communications/functionality for a desired time period. Alternatively, the user can enter a code or biometric to enable proximity PayPass chip communications/functionality for a suitably specified time period upon successful local verification by the chip. The user enters their account PIN code or biometric (e.g., via device pushbuttons), which is communicated internally or locally to the device chip via chip physical contact plates or leads. The account code PIN code or biometric is locally checked by the chip. Upon successful verification, the proximity PayPass functionality of the device is enabled by the chip, which additionally produces a unique one-time use cryptogram PIN-Flag. The one-time use cryptogram PIN-Flag, which may, for example, be up to 8 bytes long or a fraction thereof, is converted to digit format using PayPass conversion methods for display. Thus, the all-in-one device, which may be personally owned by (or issued to) an individual user, allows the user to “pre-sign” a PayPass transaction.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Further features and advantages of the disclosed subject matter will become apparent from the following detailed description taken in conjunction with the accompanying figures showing illustrative embodiments of the disclosed subject matter, in which:

FIG. 1 is a schematic illustration of an all-in-one payment device based on a non-ISO contact payment device, which is configured to additionally have

contactless payment capabilities, in accordance with the principles of the present invention. A chip card with an RF antenna provides non-contactless proximity payment capabilities.

FIG. 2 is a flow diagram illustrating exemplary steps in proximity payment transaction using local authentication features of the device of FIG.1, in accordance with the principles of the present invention.

### DESCRIPTION OF THE INVENTION

An all-in-one payment device is provided. The all-in-one payment device has operational features of both a contact payment device and a non-contact (i.e., proximity) payment device. The all-in-one payment device need not conform to ISO specifications.

The invention is described herein using MasterCard's branded PayPass proximity devices and applications as illustrative examples, with the understanding that the present invention is not limited to the examples used herein, but is also applicable to other types of payment applications, instruments or devices that may be used in proximity payment transactions.

In an embodiment of the invention shown in FIG. 1, an exemplary non-ISO device (e.g., a portable contact payment card device or token 100, FIG. 1) further includes a microelectronic chip card 110. Portable contact payment card device or token 100 may, for example, be fabricated by modifying a commercially available non-ISO device (e.g., models Xi-Sign sold by Almex Ltd., 3853 Trelawny Circle, Mississauga, Ontario, Canada L5N 6S4). Chip card 110 includes an RF antenna (e.g., a PayPass antenna) and a proximity payment application (e.g., a PayPass application) disposed on it. Further, a suitable authentication program (e.g., MasterCard's two-factor Chip Authentication Program (CAP)) is disposed on the

same chip card. The device 100 is configured for dual-mode operation (i.e., contact and contactless modes), which includes an account holder verification method based on verification of a PIN entry made via pushbutton keyboard 120. Alternatively or additionally, the device may be configured with a biometric entry for suitable  
5 biometric verification of user identity. The device may also include a feedback mechanism, which is configured to inform a user whether a verification entry (PIN or biometric) is or is not accepted by the device. An alphanumeric display 130 may provide the information visually.

Device 100 enables merchants to accept contact card transactions and  
10 contactless smartcard transactions (e.g., PayPass transactions) and can be readily integrated with existing POS, ECR or PC devices via conventional wireless or wired links (e.g., a USB link).

Advantageously, device 100 can provide a transaction that has been “pre-signed.” In a preferred embodiment of the device, this pre-signing is obtained  
15 combining the fast and easy Tap & Go payment feature of a Point of Sale PayPass application and a user authentication application that is traditionally used in non-face-to-face transaction environments (e-commerce environments). In the preferred embodiment, the latter authentication application includes robust PIN entry features and within the chip PIN validation service (e.g., CAP).

20 For PayPass POS transactions, device 100 can provide account holder authentication within the device itself. This capability advantageously eliminates the need to have the account holder enter his or her PayPass payment account PIN in a separate merchant POS Pin Pad.

FIG. 2 shows an exemplary method 200 of using device 100 for a PayPass  
25 payment to a merchant. In method 200, at step 210 the account holder enters his or

her payment account PIN code digits utilizing the PIN entry capabilities of device 100 (e.g., via pushbutton keyboard 120), before the account holder interacts with the merchant's PayPass Point of Sale (POS) device or other PayPass accepting device (step 290). At subsequent or concurrent step 220, the account holder sees (or receives  
5 other feedback) that the PIN digits entries are being received by device 100. For example, display 130 may indicate the PIN digits as they are being entered by the account holder by visual and/or audio signal. In a preferred embodiment, an asterisk is displayed for each digit of the PIN entered.

At step 230, the entered PIN code is sent to the chip in device 100 via  
10 conventional chip contact plates or leads for validation within the chip. At step 240, PayPass application functionality is enabled only if the validation at step 230 indicates that the PIN is correct. Thus, steps 230 and 240 jointly provide at the same time a secure on/off feature for proximity payment as well as the user authentication feature of a PayPass user.

15 For a preferred embodiment of process 200, the PayPass application is configured to send, at step 250, a "verification status" indicator in a standard PayPass message protocol field to the PayPass accepting device (e.g., merchant POS device). The verification status indicator informs the accepting device that device 100/PayPass chip 110 has already verified the user and has produced Cardholder Verification  
20 Results (CVR) (e.g., PIN-Flag).

The verification status indicator may, for example, have a tag, length, and value format (TLV format), similar to EMV. In a particular example, the tag element uses EMV conventions and accordingly uses the 4 characters '9F34' to indicate to the terminal that the chip has produced Cardholder Verification Results (CVR). This  
25 Cardholder Verification Results "PIN-Flag" value may be placed in any suitable or

available field portion of the PayPass or EMV “ARQC” cryptogram, which portion is then converted to display digit format according to, for example, PayPass binary display data conversion methods. It will be understood that there is no security need to encrypt this value since it is not the user’s PIN, but is only an indication that the PayPass chip card 110 itself has just verified the PIN. Unlike a compromised PIN, the indicator value itself cannot be used to establish user identity.

With renewed reference to FIG. 2, in process 200 at step 260, the merchant’s PayPass accepting device responds to the receipt of this special PIN-Flag field. The response may, for example, be any one of one of two responses A and B according to whether the tag value is an unsigned value or a digitally signed value, respectively.

Response A (unsigned value)

In a preferred embodiment, if the tag value is ‘9F34’ (which it is not a PKI based digitally signed value), the merchant’s POS device learns by receiving this “tag” value that the PayPass transaction has a “user entered and a local device (i.e., device 10) verified” PIN for the transaction. At step 262a, the merchants’ POS device sends the “flag value” to the issuer for validation. In this option, the payment device issuer can verify if the PIN-Flag value field is correct. For this purpose at step 262a, the POS terminal sends a normal online authorization message with this PIN-Flag value populated in any convenient banking network message field, for example, by using Data Element (DE) #55 (chip data) or MasterCard’s field DE #48 (UCAF data), or ISO DE 52 (PIN Data) field, or any other data field as appropriate for the network.

Response B (digitally signed value)

If the tag value is a PKI based digitally signed flag value, for example, ‘9F35’, the merchant’s POS device learns by receiving this tag value that the PayPass

transaction has a user-entered PIN value associated with the transaction and which PIN value has been verified by local device 100. Unlike the case of the unsigned values (step 262a), the signed flag value is not sent to the issuer for validation. Instead, at step 262b, the flag value is checked or verified locally within the POS device environment. For this purpose, the POS device receives the “PKI private key” signed PIN-Flag field. In a preferred embodiment, the PayPass chip card sends to the merchants’ PayPass POS reader its EMV chip card Issuer public key EMV certificate (step 261). The merchants’ PayPass POS device verifies the chip card’s Issuer public key certificate using its EMV root certificate for the account payment brand. If good, the POS device then uses the just checked chip card’s Issuer public key certificate over the signed PIN-Flag field to verify the PIN-Flag value using normal PKI signature verification techniques.

In this manner at step 262b, the merchants’ PayPass POS device locally checks or verifies offline that the PIN-Flag value is valid. If the value is valid, subsequent processing of the payment transaction can proceed as for an offline signed transaction. The merchants’ PayPass POS device also learns that it does not need to authenticate the user by prompting the user for a PIN code or signature or biometric entry.

With renewed reference to FIG. 1, it is noted that exemplary device 100 as shown is obtained by modifying a particular Xiring device (e.g., a Xiring Smart Token 1000). The Xiring devices have a battery, a display, and a general numeric entry capability for PIN entry and/or entry of additional transaction specific data. These devices also have one or more buttons (e.g., an enter key or navigation buttons), which power the device unit on or off and control the device’s operation. The commercially available Xiring 1000 device is a self-contained product that

features a Chip Authentication Program-compliant chip. A user enters his or her PIN into the device, which then creates a unique, one-time code. That code permits the user to conduct online banking or e-commerce transactions at suitably-enabled merchant sites. The one-time code that is generated, based on EMV and CAP, only  
5 works once, then becomes null upon the completion of the transaction.

To fabricate all-in-one device 100, a commercial Xiring 1000 device is modified by adding a PayPass antenna (not shown) and replacing the existing “contact only” chip in the commercial Xiring 1000 device with a dual-mode (contact and contactless) chip which supports PayPass functionality.

10 In addition to these hardware changes, optional CVM function software changes may be made to the PayPass payment application for CVM validation. The resulting device 100 is a small “CAP capable” self-powered non-card form factor device. The modified device is a combination unit with an “all-in-one” CAP device with additional PayPass functionality, which has cardholder authentication and  
15 PayPass payment ability.

All-in-one device 100 and its implementations may be backwards compatible with existing electronic payment infrastructure. Merchant terminals and PayPass readers, which are configured to process the cryptogram (i.e., a flag), will process the flag placed in the designated proximity protocol message field.  
20 Conversely, legacy terminals will ignore the designated proximity protocol message field and its contents (i.e., the flag) and otherwise process the transaction data in the usual manner.

In a preferred embodiment of this option, the cryptogram is coded in tag, length, value (TLV) format, similar to EMV. This tag (hex ‘9F34’) indicates to the  
25 merchant terminal that the chip has produced a Cardholder Verification Result (CVR).

The chip CVR cryptogram is unique for the upcoming transaction. The CVR result can be produced using other input data different from the input data used to create the PayPass cryptogram, but preferably is logically linked to the upcoming payment transaction cryptogram by using the same chip transaction counter. As another  
5 option, the CVR cryptogram may be a non-overlapping portion of a larger cryptogram used to create the PayPass cryptogram for the payment transaction.

This chip created cryptogram provides proof that the chip has completed account holder verification and the cryptogram (i.e., a flag) is passed to the PayPass reader in a convenient proximity protocol message field. This account holder  
10 verification value is subsequently sent to the card issuer in an existing 0100 authorization message field such as DE 55 (data element 55), or the MasterCard UCAF field, or the ISO DE 52 (PIN Data) field. There is no need to encrypt this CVR cryptogram indicator value since it is not the user's PIN but a verifiable (by the issuer) value which indicates that the PayPass chip has already locally verified the  
15 PIN or user provided biometric in the user device, not in any merchant point of sale equipment. Upon receiving the normal authorization message with this CVR cryptogram, it is an issuer option to verify if the value is correct.

In an alternate embodiment, dual-mode operation of the all-in-one device may exploit EMV PKI for card and PIN-Flag authentication. In this embodiment, the  
20 all-in-one device, which is associated with an EMV public key, signs the cryptogram (i.e., flag) using its private key. The EMV PayPass reader or terminal, using EMV PKI certificates and procedures, would verify or validate the signature of the particular PIN-Flag. After the validity of the signature has been validated, the device may go offline, and further transaction data processing may proceed in the usual EMV  
25 off-line manner on the basis that authorization was given by the user's smart card.

Although the present invention has been described in connection with specific exemplary embodiments, it should be understood that various changes, substitutions, and alterations apparent to those skilled in the art can be made to the disclosed embodiments without departing from the spirit and scope of the invention.

WE CLAIM:

1. A proximity payment device comprising:
  - a dual-mode (contact and contactless) chip card;
  - 5 an RF antenna and a proximity payment application disposed on chip card, the RF antenna and the proximity payment application providing proximity payment functionality;
  - a proximity payment functionality on-off mechanism;
  - at least one of a manual PIN code and biometric identifier entry device;
  - 10 and
  - a PIN code and/or biometric identifier authentication program disposed on the chip card coupled to the at least one of the manual PIN code and biometric identifier entry device.
2. The device of claim 1, wherein the proximity payment
- 15 functionality on-off mechanism is a user-operable on-off switch.
3. The device of claim 1, wherein the proximity payment functionality on-off mechanism is responsive to local or internal chip verification of entered PIN code and/or biometric identifiers for a payment transaction.
4. The device of claim 1, wherein the dual-mode card is
- 20 configured to generate a unique one-time use flag in response to successful local or internal chip verification of entered PIN code and/or biometric identifiers for a proximity payment transaction.
5. The device of claim 1, further comprising at least one of wired links and wireless links to a merchant's point-of-sale (POS) device, and wherein the

device is further configured to send an unsigned verification status indicator in a standard proximity payment message protocol over the links to the POS device.

6. The device of claim 1, further comprising at least one of wired links and wireless links to a merchant's point-of-sale (POS) device, and wherein the device is further configured to send a digitally signed verification status indicator in a standard proximity payment message protocol over the links to the POS device.

7. The device of claim 1, further comprising a display for communicating transaction information including PIN entry status and verification flags to the device user.

8. A method for conducting a proximity payment cardholder-merchant transaction, the method comprising:

before interacting with a merchant POS device, having the cardholder pre-sign (i.e., authenticate) the transaction, wherein the pre-signing comprises:

having the cardholder submit cardholder identification for local or internal verification by the proximity payment device, and in response, generating a verification status indicator by the payment card; which can be shown on the device and

interacting with a merchant POS device to communicate the verification status indicator with the transaction to the Merchant POS device.

9. The method of claim 1, wherein interacting with a merchant POS device to communicate the verification status indicator comprises sending a digitally unsigned verification status indicator value in a standard proximity payment message protocol field.

10. The method of claim 9, further comprising,

at the merchant POS device, sending the received digitally unsigned verification status indicator value to the issuer for further transaction processing.

11. The method of claim 1, wherein interacting with a merchant POS device to communicate the verification status indicator comprises sending a  
5 digitally signed verification status indicator value in a standard proximity payment message protocol field.

12. The method of claim 10, further comprising,  
at the merchant POS device, sending the received digitally unsigned verification status indicator value to the issuer for further transaction processing.

FIG. 1  
100



5

FIG. 1 All-In-One Xiring device (with on/off feature and CAP feature) having PayPass functionality. The device has a PIN CVR "indicator" to merchant POS components. The device provides a new PIN management feature and re-uses current message infrastructure where the merchant terminal receives a transaction that has

10

already been approved (signed) by the consumer.

