[0006] For example, a user may receive a token, representing an amount of currency, which he or she may present to a third-party, being a merchant, so as to enact a payment for goods received from or services received by that merchant. In another example, a mobile money token may be issued by a mobile money operator upon request by a user. The user may then present this token to a participating merchant or to a participating mobile money agent so as to redeem the token. Similarly, a user may request and subsequently communicate a token to a third party, being a friend or family member, as a remittance medium. This friend or family member may then redeem the token at a participating merchant or to a participating mobile money agent so as to redeem the token.

[0007] Oftentimes, tokens are closed-loop in that an issued token may only be redeemed at participating third-parties and may not be accepted by others. The closed-loop nature of such and other tokens is often necessitated by the fact that the tokens are often not easily formatted into conventional payment message formats and/or are not easily entered into conventional point-of-sale devices. For example, the token may not provide sufficient information to be formatted into a payment message which is communicated to a payment processing network. Furthermore, it may be difficult and expensive to modify each and every point-of-sale device for token acceptance.

[0008] In some cases, interoperability may be achieved by physically embodying the tokens on, or linking the tokens to, payment cards – often referred to as cash-cards – which provide necessary routing information and an appropriate point-of-sale device interface. However, such a solution places limitations on the ease of requesting and transferring tokens between parties and also raises costs.

[0009] These and other limitations with point-of-sale devices present problems as methods of payment develop.

BRIEF SUMMARY

[0010] In accordance with a first aspect of the invention, there is provided a payment card for use with a payment card acceptance terminal, the payment card comprising: an acceptance terminal interface component for interfacing with a payment card acceptance terminal; a user input receiving component for receiving an input by a user directly; an integrated circuit in communication with the

the user input receiving component and the acceptance terminal interface component.

[0027] Still further features provide for the integrated circuit to be a hardware security module comprising a public processor and a secure processor.

[0028] In accordance with a second aspect of the invention, there is provided a system for providing payment credentials, comprising: a payment card acceptance terminal having a card reading component; and a payment card for use with the payment card acceptance terminal including: an acceptance terminal interface component for interfacing with a payment card acceptance terminal; a user input receiving component for receiving an input by a user directly; an integrated circuit in communication with the acceptance terminal interface and the user input receiving component and configured to provide payment credentials to the payment card acceptance terminal on receipt of an input at the user input receiving component.

[0029] In accordance with a third aspect of the invention, there is provided a method carried out at an integrated circuit of a payment card comprising: receiving a user input, wherein the user input is directly received into the payment card; providing payment credentials to an acceptance terminal interface component based on the user input.

[0030] Further features provide for receiving a user input to receive a passcode and for providing payment credentials to release stored payment credentials from the payment card to the acceptance terminal interface component.

[0031] Still further features provide for receiving a user input to receive a single use account number and for providing payment credentials to provide the single use account number to the acceptance terminal interface component.

[0032] Yet further features provide for receiving a user input to receive a token and for providing payment credentials to transform the user input into formatted payment credentials.

[0033] In accordance with another aspect of the invention, there is provided a dual-interface adapter device for a payment card acceptance terminal, the dual-interface adapter device comprising: a contact-based interface insertable into a card slot of the acceptance terminal; a user interface, configured to receive power from the

acceptance terminal via the contact-based interface and to receive input from a user; and, an integrated circuit, in communication with the contact-based interface and the user interface and configured to perform cryptographic functions and translation functions; wherein the user interface is configured to receive a token from the user, and the integrated circuit is configured to decode the received token and to appropriately format information contained therein into payment credentials so that a payment card acceptance terminal can process the payment credentials.

BRIEF DESCRIPTION OF THE DRAWINGS

[0034] FIG. 1 is a schematic diagram which illustrates a system for providing payment credentials;

[0035] FIG. 2A is a schematic diagram of an exemplary system according to embodiments of the invention;

[0036] FIG. 2B is a schematic diagram of an exemplary system according to another embodiment;

[0037] FIG. 2C is a yet another schematic diagram of an exemplary system according to a further embodiment;

[0038] FIG. 3A is a block diagram which illustrates an exemplary dual-interface adapter device according to an embodiment of the invention;

[0039] FIG. 3B is a block diagram which illustrates an exemplary dual-interface adapter device according to another embodiment of the invention;

[0040] FIG. 4 is a swim-lane flow diagram which illustrates methods for providing payment credentials;

[0041] FIG. 5 is a block diagram which illustrates a system for providing payment credentials;

[0042] FIG. 6 illustrates an example of a computing device in which various aspects of the disclosure may be implemented; and,

[0043] FIG. 7 shows a block diagram of a communication device that may be used in embodiments of the disclosure.

terminal interface component of the payment card (240) is a wireless communication interface (250). Thus, the payment card (240) may be able to transmit payment credentials to the payment card acceptance terminal (242) via a wireless communication channel. As has been described in the foregoing, the payment card (240) may be configured to receive user input via a user input receiving component and, in response to receiving the user input, transmit payment credentials to the payment card acceptance terminal (242). The user input may include one of single-use payment credentials, a payment token, a personal identification number (PIN) or the like. The payment card acceptance terminal (242) may then transmit the payment credentials received from the payment card (240) to the payment processing network (210).

[0063] FIG. 3A is a schematic diagram of an exemplary payment card (300) according to some embodiments. The payment card (300) may have payment credentials stored therein or may be a dual-interface adapter device having no payment credentials stored therein. In this embodiment, the payment card (300) is in the form of a card. The size of the payment card (300) resembles the size of a credit card to allow the payment card (300) to be insertable into a payment card acceptance terminal. The payment card (300) includes an acceptance terminal interface component being a contact-based interface (320), a user input receiving component (310) being an alpha-numeric keypad, and an integrated circuit (315) being a secure element. The integrated circuit is in communication with the contact-based interface (320) and the user input receiving component (310).

[0064] The user input receiving component (310) may be any appropriate user interface, and in a preferred embodiment is an alpha-numeric keypad. Embodiments of the invention provide for the keypad to include a serial data (I/O) which performs any serialize and de-serialize functions as required, and translates data received at the user input receiving component (310) into character frames for communication to the integrated circuit (315). The data received at the user input receiving component (310) may, for example, be a token input by a user. In other embodiments, the user input receiving component (310) may be a QWERTY keypad.

[0065] In the exemplary embodiment, the contact-based interface (320) is compliant with the Europay-MasterCard-Visa (EMV) specification according to the ISO/IEC

[0068] Some of the data elements of the track 2 payment credentials may be populated with decoded information obtained from the token, such as the expiration date, for example. The integrated circuit (315) may be further configured to annex a bank identification number (BIN) to the account number to form a PAN which populates the PAN data element. The BIN may be retrieved from a digital memory of the integrated circuit (315) and may provide necessary routing information. In preferred embodiments, the service code data element is populated with a service code retrieved from the digital memory of the integrated circuit (315). In some embodiments, the decoded information does not include a CVV, in which case the integrated circuit (315) is configured to generate the CVV by, for example, encrypting one or more of the PAN, expiration date and service code with an encryption key and decimalising the result. The encryption key may be retrieved from the digital memory of the integrated circuit (315) and may be specific to an issuer of the payment (300) and/or to that specific payment card.

[0069] The integrated circuit (315) may be further configured to perform auxiliary functions such as cryptographic functions (e.g., encryption, decryption) and translation functions to adapt the payment credentials into character frames to comply with the EMV specification if required. The integrated circuit (315) may receive power (VCC and GND) and a clock signal (CLK) from the C1, C5 and C3 contact pads respectively. The integrated circuit (315) may be any suitable circuit or microprocessor and in a preferred embodiment includes a secure crypto-processor. Such an embodiment accordingly provides for the integrated circuit to be in accordance with those provided in conventional 'chip and pin' or integrated circuit (IC) credit cards. This enables end-to-end secure communications between the user input receiving component (310) and the contact-based interface (320).

[0070] Further embodiments of the invention provide for the integrated circuit (315) to be a hardware security module (HSM) which uses hardware to encrypt and decrypt data instead of solely performing the encryption/decryption in software, and accordingly provides enhanced protection over software encryption technologies. For example, the HSM might be able to provide secure key management to generate cryptographic keys, sets the capabilities and security limits of keys, implement key backup and recovery, prepare keys for storage and performs key revocation and destruction. In some embodiments, the HSM is implemented as a dual processor

device that includes a secure processor with storage and a public processor with storage. The two processors may each comprise one or more secure crypto-processors and may be identical to each other. Alternatively the secure processor may be implemented with one or more secure crypto-processors while the public processor may be implemented with one or more processors. The HSM may also include a physical or logical separation between interfaces that are used to communicate critical security parameters and other interfaces that are used to communicate other data. The HSM can also provide a tamper-proof mechanism that provides a high risk of destroying the HSM and the cryptographic keys stored therein, if any attempt is made to remove or externally access the HSM. The HSM according to embodiments of the invention may be compliant with at least a security level 2 of the FIPS 140-2 standard. Preferably, the HSM in embodiments of the invention is compliant with security level 3 or level 4 of FIPS 140-2. In some embodiments, the HSM is a packaged semiconductor chip that includes both a secure processing unit (SPU) and a public processing unit (PPU) in a single package, but with a logical and physical separation between the SPU and the PPU. In other embodiments, the SPU and the PPU can be individually packaged semiconductor chips or semiconductor dies that are coupled together to implement the HSM.

[0071] In some embodiments of the invention, the integrated circuit (315) may have payment credentials and a passcode offset stored therein. In such an embodiment, the payment credentials may only be provided to a payment card acceptance terminal upon receipt of an input in the form of a corresponding passcode at the user input receiving component (310). For example, a user wishing to provide payment credentials to a merchant so as to conduct a financial transaction, may be required to input a passcode into the payment card (300) using the user input receiving component (310). The received passcode may be transmitted from the user input receiving component (310) to the integrated circuit (315) whereupon it may be compared to the passcode offset stored therein. If the passcode matches the offset, the integrated circuit (315) may be configured to transmit the payment credentials to a payment card acceptance terminal via the contact-based interface (310). Such an embodiment may provide a payment card (300) which is configured to function as its own personal PIN entry device (PPED).

[0072] In other embodiments, single-use payment credentials may be input into the payment card (300) via the user input receiving component (310). The single-use payment credentials may be transmitted from the user input receiving component (310) to the integrated circuit (315). In some cases, the single-use payment credentials may be received in a format which is acceptable by a payment card acceptance terminal, in which case the integrated circuit (315) may transmit the received single-use payment credentials to the payment card acceptance terminal via the contact-based interface (320). In other cases, where the received single-use payment credentials are not in a format acceptable by the payment card acceptance terminal, the integrated circuit may format the received single-use payment credentials into a format which is acceptable to the payment card acceptance terminal.

[0073] FIG. 3B is a schematic diagram which illustrates an embodiment wherein the user input receiving component (312) of the payment card (301) or dual-interface adapter device is provided as a separate unit. The user interface (312) is in communication with the integrated circuit (316) via a cable (314). In other embodiments, the user interface (312) may be in wireless communication with the integrated circuit (316). Such embodiments may enable a user may hold the user interface (312) in his or her hand while entering a token.

[0074] Embodiments of the invention accordingly provide a payment card which may be compatible with any conventional card acceptance terminal, for example an EMV card acceptance terminal specified according to ISO/IEC 7816 standards, without any modifications having to be performed on that card acceptance terminal. The payment card may be inserted therein may then receive user input, for example token-based payment credentials, single-use payment credentials or a passcode. In the case of a token, token-based payment credentials may be generated by decoding token information included in the token. Embodiments of the invention provide for the token to be alphanumeric and optionally encrypted and for the payment card to be configured to decrypt the token. Encrypting the token may reduce the human readable length of the token. For example a user may read and subsequently enter a four digit token into the payment card, which when decrypted, may have a greater length. This effectively reduces the length of the token which the user enters into the payment card and my consequently reduce likelihood of errors.

Embodiments of the invention accordingly provide a device and system with which and wherein tokens may be used in an interoperable manner with third-parties, being merchants or the like, having a conventional card acceptance terminal and a connection to a payment processing network.

[0075] It will be appreciated that although FIGS. 3A and 3B illustrate embodiments wherein the payment card includes an acceptance terminal interface component in the form of a contact-based interface, portions of the description may similarly apply to embodiments wherein the acceptance terminal interface component is provided by a magnetic stripe, a wireless interface component or the like.

[0076] Use of a payment card or dual-interface adapter device of the foregoing description will now be described with reference to FIG. 4, which is a swim-lane flow diagram showing roles of various parties.

[0077] In a first step (1000), the payment card (400) is provided at a payment card acceptance terminal. In some embodiments, this may include the payment card (400) being inserted into a payment card acceptance terminal (402) while in other embodiments the payment card (400) may be brought into the vicinity of the payment card acceptance terminal (402) such that the payment card may communicate wirelessly with the card acceptance terminal (402).

[0078] When the payment card (400) is provided at a card acceptance terminal (402) the payment card (400), including the user input receiving component and integrated circuit, receives power from the card acceptance terminal (402) in a next step (1002). In some embodiments power is provided from the payment card acceptance terminal (402) to the payment card (400) through the C1 (for VCC) and C5 (for GND) contact pads. The card acceptance terminal (402) may, for example, supply a voltage in the range of 1 V to 6 V to the payment card (400). The user input receiving component draws power from the card acceptance terminal (402) through the physical connection between the payment card (400) and the card acceptance terminal (402) at the C1 and C5 contact pads when the payment card (400) is inserted into the card slot of the card acceptance terminal (402). In another embodiment, the payment card (400) may be configured to harvest power from the card acceptance terminal (402) using, for example, NFC or otherwise harvesting electromagnetic power.

WHAT IS CLAIMED IS:

1. A payment card for use with a payment card acceptance terminal, the payment card comprising:

an acceptance terminal interface component for interfacing with a payment card acceptance terminal;

a user input receiving component for receiving an input by a user directly;

an integrated circuit in communication with the acceptance terminal interface and the user input receiving component and configured to provide payment credentials to the payment card acceptance terminal on receipt of an input at the user input receiving component.

2. The payment card as claimed in claim 1, wherein the integrated circuit is configured to provide payment credentials stored on the payment card on receipt of an input in the form of a passcode at the user input receiving component.

3. The payment card as claimed in claim 1, wherein the integrated circuit is configured to provide payment credentials in the form of a single use account number received as an input at the user input receiving component.

4. The payment card as claimed in claim 1, wherein the integrated circuit is configured to provide payment credentials formatted by the integrated circuit by transforming an input in the form of a token received at the user input receiving component into the payment credentials.

5. The payment card as claimed in claim 4, wherein the integrated circuit is configured to decode the token and to appropriately format information contained therein into payment credentials, wherein the information contained in the decoded token includes an account number.

6. The payment card as claimed in claim 5, wherein the integrated circuit is configured to include a bank identification number in the payment credentials, wherein the bank identification number is retrieved from a digital memory of the integrated circuit.

7. The payment card as claimed in claim 6, wherein the integrated circuit is configured to generate a card verification value, wherein generating a card verification value encrypts at least one of received credential using an encryption key, decimalizes the result; and wherein the encryption key is retrieved from a digital memory of the integrated circuit.

8. The payment card as claimed in claim 1, wherein the user input receiving component is a keypad integrated into the payment card.

9. The payment card as claimed in claim 1, wherein the acceptance terminal interface component is a contact-based interface insertable into a card slot of the acceptance terminal; wherein the contact-based interface includes conductive contact pads for providing a contact based connection to corresponding conductive contacts of the card slot of the payment card acceptance terminal.

10. The payment card as claimed in claim 1, wherein the acceptance terminal interface component is a wireless interface component for communicating wirelessly with the payment acceptance terminal.

11. The payment card as claimed in claim 1, wherein the acceptance terminal interface component is a magnetic stripe.

12. The payment card as claimed in claim 1, wherein the user input receiving component is configured to receive or harvest power from the card acceptance terminal.

13. The payment card as claimed in claim 1, wherein the integrated circuit is a secure crypto-processor configured to perform cryptographic functions and translation functions.

14. The payment card as claimed in claim 13, wherein the secure crypto-processor enables end-to-end secure communications between the user input receiving component and the acceptance terminal interface component.

15. The payment card as claimed in claim 1, wherein the integrated circuit is a hardware security module comprising a public processor and a secure processor.

16. A system for providing payment credentials, comprising:

a payment card acceptance terminal having a card reading component; and

a payment card for use with the payment card acceptance terminal including:

an acceptance terminal interface component for interfacing with a payment card acceptance terminal;

a user input receiving component for receiving an input by a user directly;

an integrated circuit in communication with the acceptance terminal interface and the user input receiving component and configured to provide payment credentials to the payment card acceptance terminal on receipt of an input at the user input receiving component.

17. A method carried out at an integrated circuit of a payment card comprising:

receiving a user input, wherein the user input is directly received into the payment card;

providing payment credentials to an acceptance terminal interface component based on the user input.

18. The method as claimed in claim 17, wherein receiving a user input receives a passcode and providing payment credentials releases stored payment credentials from the payment card to the acceptance terminal interface component.

19. The method as claimed in claim 17, wherein receiving a user input receives a single use account number and providing payment credentials provides the single use account number to the acceptance terminal interface component.

20. The method as claimed in claim 17, wherein receiving a user input receives a token and providing payment credentials transforms the user input into formatted payment credentials.

[0006] For example, a user may receive a token, representing an amount of currency, which he or she may present to a third-party, being a merchant, so as to enact a payment for goods received from or services received by that merchant. In another example, a mobile money token may be issued by a mobile money operator upon request by a user. The user may then present this token to a participating merchant or to a participating mobile money agent so as to redeem the token. Similarly, a user may request and subsequently communicate a token to a third party, being a friend or family member, as a remittance medium. This friend or family member may then redeem the token at a participating merchant or to a participating mobile money agent so as to redeem the token.

[0007] Oftentimes, tokens are closed-loop in that an issued token may only be redeemed at participating third-parties and may not be accepted by others. The closed-loop nature of such and other tokens is often necessitated by the fact that the tokens are often not easily formatted into conventional payment message formats and/or are not easily entered into conventional point-of-sale devices. For example, the token may not provide sufficient information to be formatted into a payment message which is communicated to a payment processing network. Furthermore, it may be difficult and expensive to modify each and every point-of-sale device for token acceptance.

[0008] In some cases, interoperability may be achieved by physically embodying the tokens on, or linking the tokens to, payment cards – often referred to as cash-cards – which provide necessary routing information and an appropriate point-of-sale device interface. However, such a solution places limitations on the ease of requesting and transferring tokens between parties and also raises costs.

[0009] These and other limitations with point-of-sale devices present problems as methods of payment develop.

BRIEF SUMMARY

[0009a] The invention is defined in the independent claims. Some optional features of the invention are defined in the dependent claims.

[0010] In accordance with a first exemplary technique, there is provided a payment card for use with a payment card acceptance terminal, the payment card comprising: an acceptance terminal interface component for interfacing with a payment card acceptance terminal; a user input receiving component for receiving an input by a user directly; an integrated circuit in communication with the

the user input receiving component and the acceptance terminal interface component.

[0027] Still further features provide for the integrated circuit to be a hardware security module comprising a public processor and a secure processor.

[0028] In accordance with a second exemplary technique, there is provided a system for providing payment credentials, comprising: a payment card acceptance terminal having a card reading component; and a payment card for use with the payment card acceptance terminal including: an acceptance terminal interface component for interfacing with a payment card acceptance terminal; a user input receiving component for receiving an input by a user directly; an integrated circuit in communication with the acceptance terminal interface and the user input receiving component and configured to provide payment credentials to the payment card acceptance terminal on receipt of an input at the user input receiving component.

[0029] In accordance with a third exemplary technique, there is provided a method carried out at an integrated circuit of a payment card comprising: receiving a user input, wherein the user input is directly received into the payment card; providing payment credentials to an acceptance terminal interface component based on the user input.

[0030] Further features provide for receiving a user input to receive a passcode and for providing payment credentials to release stored payment credentials from the payment card to the acceptance terminal interface component.

[0031] Still further features provide for receiving a user input to receive a single use account number and for providing payment credentials to provide the single use account number to the acceptance terminal interface component.

[0032] Yet further features provide for receiving a user input to receive a token and for providing payment credentials to transform the user input into formatted payment credentials.

[0033] In accordance with another exemplary technique, there is provided a dual-interface adapter device for a payment card acceptance terminal, the dual-interface adapter device comprising: a contact-based interface insertable into a card slot of the acceptance terminal; a user interface, configured to receive power from the

acceptance terminal via the contact-based interface and to receive input from a user; and, an integrated circuit, in communication with the contact-based interface and the user interface and configured to perform cryptographic functions and translation functions; wherein the user interface is configured to receive a token from the user, and the integrated circuit is configured to decode the received token and to appropriately format information contained therein into payment credentials so that a payment card acceptance terminal can process the payment credentials.

BRIEF DESCRIPTION OF THE DRAWINGS

[0034] FIG. 1 is a schematic diagram which illustrates a system for providing payment credentials;

[0035] FIG. 2A is a schematic diagram of an exemplary system;

[0036] FIG. 2B is a schematic diagram of an exemplary system;

[0037] FIG. 2C is a yet another schematic diagram of an exemplary system;

[0038] FIG. 3A is a block diagram which illustrates an exemplary dual-interface adapter device;

[0039] FIG. 3B is a block diagram which illustrates an exemplary dual-interface adapter device;

[0040] FIG. 4 is a swim-lane flow diagram which illustrates methods for providing payment credentials;

[0041] FIG. 5 is a block diagram which illustrates a system for providing payment credentials;

[0042] FIG. 6 illustrates an example of a computing device in which various aspects of the disclosure may be implemented; and,

[0043] FIG. 7 shows a block diagram of a communication device that may be used in embodiments of the disclosure.

terminal interface component of the payment card (240) is a wireless communication interface (250). Thus, the payment card (240) may be able to transmit payment credentials to the payment card acceptance terminal (242) via a wireless communication channel. As has been described in the foregoing, the payment card (240) may be configured to receive user input via a user input receiving component and, in response to receiving the user input, transmit payment credentials to the payment card acceptance terminal (242). The user input may include one of single-use payment credentials, a payment token, a personal identification number (PIN) or the like. The payment card acceptance terminal (242) may then transmit the payment credentials received from the payment card (240) to the payment processing network (210).

[0063] FIG. 3A is a schematic diagram of an exemplary payment card (300) according to some embodiments. The payment card (300) may have payment credentials stored therein or may be a dual-interface adapter device having no payment credentials stored therein. In this embodiment, the payment card (300) is in the form of a card. The size of the payment card (300) resembles the size of a credit card to allow the payment card (300) to be insertable into a payment card acceptance terminal. The payment card (300) includes an acceptance terminal interface component being a contact-based interface (320), a user input receiving component (310) being an alpha-numeric keypad, and an integrated circuit (315) being a secure element. The integrated circuit is in communication with the contact-based interface (320) and the user input receiving component (310).

[0064] The user input receiving component (310) may be any appropriate user interface, and in a preferred embodiment is an alpha-numeric keypad. Exemplary arrangements provide for the keypad to include a serial data (I/O) which performs any serialize and de-serialize functions as required, and translates data received at the user input receiving component (310) into character frames for communication to the integrated circuit (315). The data received at the user input receiving component (310) may, for example, be a token input by a user. In other embodiments, the user input receiving component (310) may be a QWERTY keypad.

[0065] In the exemplary embodiment, the contact-based interface (320) is compliant with the Europay-MasterCard-Visa (EMV) specification according to the ISO/IEC

[0068] Some of the data elements of the track 2 payment credentials may be populated with decoded information obtained from the token, such as the expiration date, for example. The integrated circuit (315) may be further configured to annex a bank identification number (BIN) to the account number to form a PAN which populates the PAN data element. The BIN may be retrieved from a digital memory of the integrated circuit (315) and may provide necessary routing information. In preferred embodiments, the service code data element is populated with a service code retrieved from the digital memory of the integrated circuit (315). In some embodiments, the decoded information does not include a CVV, in which case the integrated circuit (315) is configured to generate the CVV by, for example, encrypting one or more of the PAN, expiration date and service code with an encryption key and decimalising the result. The encryption key may be retrieved from the digital memory of the integrated circuit (315) and may be specific to an issuer of the payment (300) and/or to that specific payment card.

[0069] The integrated circuit (315) may be further configured to perform auxiliary functions such as cryptographic functions (e.g., encryption, decryption) and translation functions to adapt the payment credentials into character frames to comply with the EMV specification if required. The integrated circuit (315) may receive power (VCC and GND) and a clock signal (CLK) from the C1, C5 and C3 contact pads respectively. The integrated circuit (315) may be any suitable circuit or microprocessor and in a preferred embodiment includes a secure crypto-processor. Such an embodiment accordingly provides for the integrated circuit to be in accordance with those provided in conventional ‘chip and pin’ or integrated circuit (IC) credit cards. This enables end-to-end secure communications between the user input receiving component (310) and the contact-based interface (320).

[0070] Further exemplary arrangements provide for the integrated circuit (315) to be a hardware security module (HSM) which uses hardware to encrypt and decrypt data instead of solely performing the encryption/decryption in software, and accordingly provides enhanced protection over software encryption technologies. For example, the HSM might be able to provide secure key management to generate cryptographic keys, sets the capabilities and security limits of keys, implement key backup and recovery, prepare keys for storage and performs key revocation and destruction. In some embodiments, the HSM is implemented as a dual processor

device that includes a secure processor with storage and a public processor with storage. The two processors may each comprise one or more secure crypto-processors and may be identical to each other. Alternatively the secure processor may be implemented with one or more secure crypto-processors while the public processor may be implemented with one or more processors. The HSM may also include a physical or logical separation between interfaces that are used to communicate critical security parameters and other interfaces that are used to communicate other data. The HSM can also provide a tamper-proof mechanism that provides a high risk of destroying the HSM and the cryptographic keys stored therein, if any attempt is made to remove or externally access the HSM. The HSM may be compliant with at least a security level 2 of the FIPS 140-2 standard. Preferably, the HSM is compliant with security level 3 or level 4 of FIPS 140-2. In some embodiments, the HSM is a packaged semiconductor chip that includes both a secure processing unit (SPU) and a public processing unit (PPU) in a single package, but with a logical and physical separation between the SPU and the PPU. In other embodiments, the SPU and the PPU can be individually packaged semiconductor chips or semiconductor dies that are coupled together to implement the HSM.

[0071] In some exemplary arrangements, the integrated circuit (315) may have payment credentials and a passcode offset stored therein. In such an embodiment, the payment credentials may only be provided to a payment card acceptance terminal upon receipt of an input in the form of a corresponding passcode at the user input receiving component (310). For example, a user wishing to provide payment credentials to a merchant so as to conduct a financial transaction, may be required to input a passcode into the payment card (300) using the user input receiving component (310). The received passcode may be transmitted from the user input receiving component (310) to the integrated circuit (315) whereupon it may be compared to the passcode offset stored therein. If the passcode matches the offset, the integrated circuit (315) may be configured to transmit the payment credentials to a payment card acceptance terminal via the contact-based interface (310). Such an embodiment may provide a payment card (300) which is configured to function as its own personal PIN entry device (PPED).

[0072] In other embodiments, single-use payment credentials may be input into the payment card (300) via the user input receiving component (310). The single-use payment credentials may be transmitted from the user input receiving component (310) to the integrated circuit (315). In some cases, the single-use payment credentials may be received in a format which is acceptable by a payment card acceptance terminal, in which case the integrated circuit (315) may transmit the received single-use payment credentials to the payment card acceptance terminal via the contact-based interface (320). In other cases, where the received single-use payment credentials are not in a format acceptable by the payment card acceptance terminal, the integrated circuit may format the received single-use payment credentials into a format which is acceptable to the payment card acceptance terminal.

[0073] FIG. 3B is a schematic diagram which illustrates an embodiment wherein the user input receiving component (312) of the payment card (301) or dual-interface adapter device is provided as a separate unit. The user interface (312) is in communication with the integrated circuit (316) via a cable (314). In other embodiments, the user interface (312) may be in wireless communication with the integrated circuit (316). Such embodiments may enable a user may hold the user interface (312) in his or her hand while entering a token.

[0074] Exemplary techniques accordingly provide a payment card which may be compatible with any conventional card acceptance terminal, for example an EMV card acceptance terminal specified according to ISO/IEC 7816 standards, without any modifications having to be performed on that card acceptance terminal. The payment card may be inserted therein may then receive user input, for example token-based payment credentials, single-use payment credentials or a passcode. In the case of a token, token-based payment credentials may be generated by decoding token information included in the token. Exemplary techniques provide for the token to be alphanumeric and optionally encrypted and for the payment card to be configured to decrypt the token. Encrypting the token may reduce the human readable length of the token. For example a user may read and subsequently enter a four digit token into the payment card, which when decrypted, may have a greater length. This effectively reduces the length of the token which the user enters into the payment card and my consequently reduce likelihood of errors.

Exemplary techniques accordingly provide a device and system with which and wherein tokens may be used in an interoperable manner with third-parties, being merchants or the like, having a conventional card acceptance terminal and a connection to a payment processing network.

[0075] It will be appreciated that although FIGS. 3A and 3B illustrate embodiments wherein the payment card includes an acceptance terminal interface component in the form of a contact-based interface, portions of the description may similarly apply to embodiments wherein the acceptance terminal interface component is provided by a magnetic stripe, a wireless interface component or the like.

[0076] Use of a payment card or dual-interface adapter device of the foregoing description will now be described with reference to FIG. 4, which is a swim-lane flow diagram showing roles of various parties.

[0077] In a first step (1000), the payment card (400) is provided at a payment card acceptance terminal. In some embodiments, this may include the payment card (400) being inserted into a payment card acceptance terminal (402) while in other embodiments the payment card (400) may be brought into the vicinity of the payment card acceptance terminal (402) such that the payment card may communicate wirelessly with the card acceptance terminal (402).

[0078] When the payment card (400) is provided at a card acceptance terminal (402) the payment card (400), including the user input receiving component and integrated circuit, receives power from the card acceptance terminal (402) in a next step (1002). In some embodiments power is provided from the payment card acceptance terminal (402) to the payment card (400) through the C1 (for VCC) and C5 (for GND) contact pads. The card acceptance terminal (402) may, for example, supply a voltage in the range of 1 V to 6 V to the payment card (400). The user input receiving component draws power from the card acceptance terminal (402) through the physical connection between the payment card (400) and the card acceptance terminal (402) at the C1 and C5 contact pads when the payment card (400) is inserted into the card slot of the card acceptance terminal (402). In another embodiment, the payment card (400) may be configured to harvest power from the card acceptance terminal (402) using, for example, NFC or otherwise harvesting electromagnetic power.

WHAT IS CLAIMED IS:

1. A payment card for use with a payment card acceptance terminal, the payment card comprising:

an acceptance terminal interface component for interfacing with a payment card acceptance terminal;

a user input receiving component for receiving a user input by a user directly; and

an integrated circuit in communication with the acceptance terminal interface component and the user input receiving component and configured to perform one of processing the user input as payment credentials, retrieving payment credentials stored by the payment card based on the user input, or generating payment credentials based on the user input and subsequently provide the payment credentials to the payment card acceptance terminal on receipt of the user input at the user input receiving component.

2. The payment card as claimed in claim 1, wherein the integrated circuit is configured to provide payment credentials stored on the payment card on receipt of the user input in the form of a passcode at the user input receiving component.

3. The payment card as claimed in claim 1, wherein the integrated circuit is configured to provide payment credentials in the form of a single use account number received as the user input at the user input receiving component.

4. The payment card as claimed in claim 1, wherein the integrated circuit is configured to provide payment credentials formatted by the integrated circuit by transforming the user input in the form of a token received at the user input receiving component into the payment credentials.

5. The payment card as claimed in claim 4, wherein the integrated circuit is configured to decode the token and to appropriately format information contained therein into payment credentials, and for the information contained in the decoded token to include an account number.

6. The payment card as claimed in claim 4 or claim 5, wherein the integrated circuit is configured to include a bank identification number in the payment credentials, and for the bank identification number to be retrieved from a digital memory of the integrated circuit.

7. The payment card as claimed in any one of claims 4 to 6, wherein the integrated circuit is configured to generate a card verification value, the card verification value being for encrypting one or more of a primary account number, expiration date and service code using an encryption key and for decimalizing the result, and wherein the integrated circuit is configured to retrieve the encryption key from a digital memory of the integrated circuit.

8. The payment card as claimed in any one of the preceding claims, wherein the user input receiving component is a keypad integrated into the payment card.

9. The payment card as claimed in any one of the preceding claims, wherein the acceptance terminal interface component is a contact-based interface insertable into a card slot of the payment card acceptance terminal; wherein the contact-based interface includes conductive contact pads for providing a contact-based connection to corresponding conductive contacts of the card slot of the payment card acceptance terminal.

10. The payment card as claimed in any one of claims 1 to 8, wherein the acceptance terminal interface component is a wireless interface component for communicating wirelessly with the payment card acceptance terminal.

11. The payment card as claimed in any one of claims 1 to 8, wherein the acceptance terminal interface component is a magnetic stripe.

12. The payment card as claimed in any one of the preceding claims, wherein the user input receiving component is configured to receive or harvest power from the payment card acceptance terminal.

13. The payment card as claimed in any one of the preceding claims, wherein the integrated circuit is a secure crypto-processor configured to perform cryptographic functions and translation functions.

14. The payment card as claimed in claim 13, wherein the secure crypto-processor is configured to enable end-to-end secure communications between the user input receiving component and the acceptance terminal interface component.

15. The payment card as claimed in any one of the preceding claims, wherein the integrated circuit is a hardware security module comprising a public processor and a secure processor.

16. A system for providing payment credentials, comprising:

a payment card acceptance terminal having a card reading component; and

a payment card for use with the payment card acceptance terminal including:

an acceptance terminal interface component for interfacing with a payment card acceptance terminal;

a user input receiving component for receiving a user input by a user directly; and

an integrated circuit in communication with the acceptance terminal interface component and the user input receiving component and configured to perform one of processing the user input as payment credentials, retrieving payment credentials stored by the payment card based on the user input, or generating payment credentials based on the user input and subsequently provide the payment credentials to the payment card acceptance terminal on receipt of the user input at the user input receiving component.

17. A method carried out at an integrated circuit of a payment card comprising:

receiving a user input, wherein the user input is directly received into the payment card;

performing one of processing the user input as payment credentials, retrieving payment credentials stored by the payment card based on the user input, or generating payment credentials based on the user input; and

providing the payment credentials to a payment card acceptance terminal.

18. The method as claimed in claim 17, wherein receiving the user input comprises receiving a passcode and providing payment credentials comprises releasing stored payment credentials from the payment card to an acceptance terminal interface component of the payment card.

19. The method as claimed in claim 17, wherein receiving the user input comprises receiving a single use account number and providing payment credentials comprises providing the single use account number to an acceptance terminal interface component of the payment card.

20. The method as claimed in claim 17, wherein receiving the user input comprises receiving a token and providing payment credentials comprises transforming the user input into formatted payment credentials and providing the formatted payment credentials to an acceptance terminal interface component of the payment card.