METHOD AND SYSTEM FOR AUTHORISING TRANSACTIONS

Technical Field

[0001] The present disclosure relates to a computer-implemented method and a system for authorising transactions, including in one or more examples, to a computer-implemented method and a system for authorising transactions using biometric authentication.

Background

[0002] Financial transactions may be conducted with cash, or in a cashless manner. For example, at an electronic transaction device, such as a point-of-sale (POS) machine, a financial card may be used for making payments instead of using cash. Recently, mobile payment and mobile transactions have also been developed, whereby a mobile computing device, such as a mobile phone or smartwatch, can be used to make payment or other types of financial transactions. This may be conducted by, e.g., using a mobile application for conducting financial transactions installed and executing on the mobile computing device.

[0003] While cashless transactions are being used more frequently nowadays, concerns have been raised regarding the security of cashless payments. For example, it has been known for card holders to suffer financial loss due to unauthorised use of lost or stolen bank cards. Users of mobile payment systems are also at risk of by attackers targeting the mobile payment system and stealing the user's personal information.

[0004] Various techniques have been developed for enhancing the security of cashless transactions. For example, when conducting a transaction using a financial card on a point-of-sale (POS) machine, the card user may be required to input a Personal Identification Number (PIN) associated with the card to prove their identity. Many mobile payment applications also allow the user to set a password or PIN for authorising transactions.

[0005] It has been proposed that biometric authentication techniques may be used in authorising transactions, e.g., by comparing captured biometric features of a person with

stored biometric template associated with the owner of the financial account used for the transaction. This approach has been considered to be securer than password-based or PIN-based authentication techniques, as the biometric features of a person are generally more difficult to steal or forge by a third party.

[0006] However, transmitting a person's biometric template to or storing it at an electronic transaction device, such as a POS machine, may lead to the risk of leaking the person's biometric template, e.g., to an attacker sniffing the data communication to the POS machine.

[0007] It is desired to address or ameliorate one or more disadvantages or limitations associated with the prior art, or to at least provide a useful alternative.

Summary

[0008] In a first aspect, there is provided a transaction device configured for processing transactions, the device including at least one processor configured to:

receive, from a payment device, one or more payment credentials and at least one device address of a companion device associated with the payment device, wherein the payment device is a payment card, wherein the companion device is a mobile device;

establish, a wireless connection with the companion device using the at least one device address;

receive, via the wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication; and

process a transaction request based on the one or more payment credentials and the biometric authentication result.

[0009] In a second aspect, there is provided a data-processor implemented method for processing transactions for a transaction device, the method including the steps of:

receiving, from a payment device, one or more payment credentials and at least one device address of a companion device associated with the payment device, wherein the payment device is a payment card, wherein the companion device is a mobile device;

establishing, a wireless connection with the companion device using the at least one device address;

receiving, via the wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication; and

processing a transaction request based on the one or more payment credentials and the biometric authentication result.

[0010] In a third aspect, there is provided a payment device configured for processing transactions, the device including at least one processor configured to:

transmit, to a transaction device for processing transactions, one or more payment credentials and at least one device address of a companion device associated with the payment device, wherein the payment device is a payment card, wherein the companion device is a mobile device; and

transmit, via a wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication.

[0011] In a fourth aspect, there is provided a data-processor implemented method for processing transactions, the method including the steps of:

transmitting, to a transaction device for processing transactions, one or more payment credentials and at least one device address of a companion device associated with the payment device, wherein the payment device is a payment card, wherein the companion device is a mobile device; and

transmitting, to the transaction device for processing transactions, via a wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication.

[0012] In a final aspect, there is provided a non-transitory computer readable storage medium embodying thereon a program of computer readable instructions which, when executed by one or more processors of a payment device in communication with at least one companion device, cause the payment device to carry out a method for processing transactions, wherein the payment device is a payment card, wherein the companion device is a mobile device, the method embodying the steps of:

transmitting, to a transaction device for processing transactions, one or more payment credentials and at least one device address of a companion device associated with the payment device; and

transmitting, to the transaction device for processing transactions, via a wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication.

Brief Description of the Drawings

[0013] Some embodiments of the present invention are hereinafter further described, by way of example only, with reference to the accompanying drawings, in which:

[0014] FIG. 1 is a schematic diagram of an example of a system for authorising transactions;

[0015] FIG. 2 is an exemplary working flow for authorising transactions implemented by the electronic transaction device 110 of FIG. 1;

[0016] FIG. 3 is an exemplary working flow for authorising transactions implemented by the mobile computing device 130 of FIG. 1;

[0017] FIG. 4 is a schematic diagram of another example of the system for authorising transactions;

[0018] FIG. 5 is schematic diagram of a payment network 140 / 440 of FIG. 1 and FIG. 4;

[0019] FIG. 6 is a detailed exemplary working flow for authorising transactions;

[0020] FIG. 7 is a schematic diagram of an example of an electronic transaction device 110 / 410 of FIG. 1 and FIG. 4; and

[0021] FIG. 8 is a schematic diagram of an example of a mobile computing device 130 / 430 of FIG. 1 and FIG. 4.

Detailed Description

[0022] Described herein is a method and system for authorising transactions using biometric authentication techniques. In the provided system, authentication of biometric features of the user is performed on an electronic device referred to as the “companion device”, rather than the electronic transaction device (e.g., a POS machine). The result of the biometric authentication is then sent by the companion device to the transaction device, e.g., via Bluetooth connection. In this way, the biometric template of the user does not need to be transmitted to or stored on the electronic transaction device, which enhances the security of the transaction authorisation process.

[0023] In this disclosure, the term “electronic transaction device”, also referred to as “transaction device”, is intended to include various electronic devices that can be used to perform cashless transactions. Such electronic transaction devices may include, e.g., a point-of-sale (POS) machine (also referred to as a POS terminal), an automated teller machine (ATM), an automated ticket machine, and any other suitable payment acceptance devices.

[0024] The term "user" is intended to refer to a person or entity wishing to conduct a transaction at an electronic transaction device, such as a point-of-sale (POS) machine, by using a financial account, e.g., a financial account associated with a bank card. The user may also be referred to as the “card holder” or the “account holder”.

[0025] The term "user account" is intended to refer to the financial account used by the user in the transaction.

[0026] The term “card”, also referred to as “financial card” or "payment card", is intended to include various cards issued by banks and other financial institutions that can be used to perform financial transactions, including but not limited to debit cards, credit cards, and other suitable payment cards.

[0027] The term “transaction” is intended to include various financial transactions that are associated with user accounts and that can be conducted through an electronic transaction device, including e.g., bill or fee payment, cash withdrawal, or account balance check.

[0028] An example of a system 100 for authorising transactions will now be described with reference to FIG. 1.

[0029] The system 100 includes an electronic transaction device in the form of a point-of-sale (POS) machine 110, a financial card 120, a companion device 130, and a payment network 140.

[0030] The POS machine 110 is in communication with the financial card 120, the companion device 130, and the payment network 140 respectively, via one or more communication networks.

[0031] In this example, the financial transaction is a payment transaction, being conducted by the user 150 at the POS machine 110 using the financial card 120. For example, the user may insert the card 120 into a card slot of the POS machine 110, or swipe the card 120 through a card-reader of the POS machine 110. In some other embodiment, both the card 120 and the POS machine 110 may have a Near Field Communication (NFC) module, and the transaction may be initiated by the user presenting the card 120 close to a NFC sensor of the POS machine 110.

[0032] The companion device 130 is a device that can perform biometric authentication of one or more of the user’s biometric characteristics, such as one or more of the following:

fingerprint, iris, and face. In this example, the companion device 130 takes the form of a mobile device, e.g., a smart phone device.

[0033] Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs).

[0034] In the embodiments described herein, both the POS machine 110 and the companion device 130 include a Bluetooth communication module for performing Bluetooth communication. In other embodiments, it should be appreciated that other forms of wireless communication can be carried out between the POS machine 110 and the companion device 130. Examples of the other forms of wireless communication can include, near field communications (NFC), WiFi, Zigbee, and so forth. In some embodiments, it is possible that Bluetooth is a primary form of wireless communication being used, while the other forms of wireless communication are used as a back-up solution if the primary form of wireless communication fails.

[0035] The Bluetooth address of the companion device 130 is stored in an internal memory of the card 120, and is sent from the card 120 to the POS machine 110 when the user 150 initiates the transaction at the POS machine 110 using the card 120. Alternatively, the Bluetooth address of the companion device 130 is sent from the companion device 130 by an application (typically a payment application) executing on the companion device 130 when the user 150 initiates the transaction at the POS machine 110 using the card 120. The Bluetooth address of the companion device 130 may be sent to the POS machine 110 by wired or wireless data communication, e.g., NFC, WiFi, Zigbee, and so forth.

[0036] In some embodiments, multiple Bluetooth addresses of respective companion devices 130 are stored in the internal memory of the card 120. In those embodiments, if a connection attempt using the first Bluetooth address fails, subsequent connection attempts are subsequently carried out using at least one of the multiple Bluetooth addresses of respective companion devices 130. It should be noted that this caters for situations where back-up companion devices 130 can be used when a primary companion device 130 has failed or is not available.

[0037] Using the received Bluetooth address, the POS machine 110 establishes a Bluetooth connection with the companion device 130.

[0038] The companion device 130 then invokes a biometric authentication process to verify one or more of the user's biometric characteristic. The biometric authentication may be performed by:

capturing one or more biometric characteristics of the user, e.g., one or more of the following: fingerprint, iris, voice and face; and

comparing the captured biometric characteristics with the biometric characteristics included in a biometric template stored in the companion device 130.

[0039] In some embodiments, after the Bluetooth connection is established using typical methods of Bluetooth pairing (for example, by determining if numerals depicted on both the POS machine 110 and the companion device 130 match one another), the POS machine 110 performs an authentication step for authenticating the companion device 130, to ensure that the device with which the POS machine is connected via Bluetooth is the correct companion device 130. This authentication step may be performed by, e,g,. the user inputting a Personal Identification Number (PIN) on the companion device 130, or performing an input as instructed by the POS machine 110.

[0040] When the biometric authentication has been completed, the result - which represents whether the captured biometric characteristics matches biometric characteristics in the stored biometric template – is then sent by the companion device 130 to the POS machine 110 via Bluetooth.

[0041] Based on the biometric authentication result received from the companion device 130, the POS machine 110 processes the payment transaction, e.g., by sending a transaction request to a payment network 140 if the biometric authentication is successful.

[0042] FIG. 2 illustrates an example of a computer-implemented method 200 for authorising transactions implemented by the POS machine 110 of FIG. 1.

[0043] As shown in FIG. 2, at Step 210, the POS machine 110 receives a Bluetooth address of a companion device 130 either from the card 120 or from the companion device 130.

[0044] Using this Bluetooth address, the POS machine 110 establishes a Bluetooth connection with the companion device 130 at Step 220.

[0045] The companion device 130 then performs the biometric authentication. When the biometric authentication has been completed, the companion device 130 sends the result to the POS machine 110 via Bluetooth.

[0046] Upon receiving the biometric authentication result from the companion device 130 via Bluetooth at Step 230, the POS machine 110 then proceeds to Step 240 to process the transaction based on the received biometric authentication result.

[0047] FIG. 3 illustrates an exemplary process for authorising transactions executed by the companion device 130.

[0048] At step 310, the companion device 130 connects with a transaction device via Bluetooth. In this example, the transaction device is the POS machine 110.

[0049] Next, the companion device 130 invokes a biometric authentication process, and captures one or more biometric characteristics of the user at Step 320. The biometric characteristics may include one or more of the following: fingerprint, iris, and face. The biometric characteristics may be captured using known techniques. For example, when the biometric characteristic includes fingerprint, it may be captured by taking a digital image of the user's fingerprint. In another example, the biometric characteristic may be facial features of the user, which can be captured by, e.g., the user taking a photo of himself / herself using the companion device 130.

[0050] At Step 330, the companion device 130 retrieves a stored biometric template of the user. The biometric template is stored in a data store of the companion device 130. The biometric template includes the user's biometric characteristics, which may be provided by the user during a registration process to the transaction authentication service.

[0051] Next, at Step 340, the companion device 130 compares the captured biometric characteristics with the biometric characteristics stored in the biometric template.

[0052] Finally, at Step 350, a biometric authentication result representing the comparison result is sent via Bluetooth to the transaction device, which is the POS machine 110 in this example.

[0053] FIG. 4 illustrates another example 400 of the system for authorising transactions. In this example, the user 420 initiates the payment transaction at the electronic transaction device in the form of POS machine 410, by using the mobile computing device 430. For example, the payment transaction may be initiated by a mobile payment application installed and executed on the mobile computing device 430.

[0054] In some embodiments, both the mobile computing device 430 and the POS machine 410 have a Near Field Communication (NFC) module, the mobile payment application may send a transaction initiating signal to the POS machine 410 through NFC, e.g., by the user presenting the mobile computing device 430 close to a NFC sensor of the POS machine 410.

[0055] Alternatively, the mobile payment application may send a transaction initiating signal to the POS machine 410 through a mobile payment server 450 with which both the mobile computing device 430 and the POS machine 410 are in communication, as shown by the dashed arrows in FIG. 4.

[0056] In this example, the mobile computing device 430 also functions as the companion device using which biometric authentication of the user 420 is performed.

[0057] The biometric authentication result, generated by the mobile computing device 430, is sent back to the POS machine 410, e.g., via Bluetooth. Both the POS machine 410 and the mobile computing device 430 have a Bluetooth communication module for performing Bluetooth communication. The mobile computing device 430 carries its own Bluetooth address, e.g., by storing the Bluetooth address in an internal or external memory.

[0058] In order to establish the Bluetooth connection for sending the biometric authentication result, the mobile computing device 430 sends the Bluetooth address to the POS machine

410, e.g., by wired or wireless connection between the mobile computing device 430 and the POS machine 410, such as NFC.

[0059] Using the Bluetooth address received from the mobile computing device 430, the POS machine 410 establishes a Bluetooth connection with the mobile computing device 430.

[0060] The mobile computing device 430 then invokes a biometric authentication process to verify the user's identity. The biometric authentication may include capturing one or more of the user's biometric characteristics, e.g., one or more of the following: fingerprint, iris, voice and face, and comparing the captured biometric characteristics with the biometric characteristics included in a biometric template stored in the mobile computing device 430.

[0061] When the biometric authentication has been completed, the mobile computing device 430 then sends the result, which represents whether the captured biometric characteristics matches the stored biometric template, to the POS machine 410, via the established Bluetooth connection.

[0062] Based on the biometric authentication result received from the mobile computing device 430, the POS machine 410 processes the payment transaction, e.g., by sending a transaction request to a payment network 440 if the biometric authentication is successful.

[0063] An exemplary structure of the payment network 140 of FIG. 1 and 440 of FIG. 4 is illustrated in FIG. 5.

[0064] The POS machine 110 / 410 is in communication with, via a communication network 510, an acquirer server 520, which in turn communicates with a payment network server 540 via a communication network 530.

[0065] The acquirer server 520 is associated with a financial institution that owns or operates the POS machine 110 / 410 on which the transaction is conducted. This financial institution may be referred to as the "acquirer", "acquiring bank", or "merchant's bank". In a payment system, the acquirer server 520 may also be referred to as the "acquirer switch".

[0066] The payment network server 540 is associated with a payment network service provider that owns or operates the payment network, such as MasterCard, Visa, American Express, PLUS, etc.

[0067] Further, via a communication network 550, the payment network server 540 is in communication with an issuer server 560 associated with a financial institution that has issued the financial account used in the transaction. This financial institution may be referred to as the "issuer" of the financial account. In a payment system, the issuer server 560 may also be referred to as the "issuer switch".

[0068] When the user makes a payment at the POS machine 110 / 410, the POS machine sends the transaction request including the user's account information and details of the payment to the acquirer server 520.

[0069] Upon receiving the transaction request from the POS machine 110 / 410, the acquirer server 520 submits the transaction request to the payment network server 540, and requests the payment network server 540 to obtain an authorization from the issuing financial institution of the user's account.

[0070] Based on the user's account information, the payment network server 540 routes the transaction request to the issuer server 560 associated with the issuing financial institution for authorization.

[0071] Based on the user's account information, the issuer server 560 determines whether to authorise the transaction, e.g., by checking if a biometric authentication process carried out with a companion device as described in the preceding sections provided a positive match/result, by checking an account balance of the user's account, and so forth. The issuer server 560 sends the authorisation result back to the payment network server 540.

[0072] The payment network server 540 then returns to the acquirer server 520 the authorisation result indicating whether the transaction request has been approved by the issuer server 560.

[0073] The acquirer server 520 then passes the authorisation result to the POS machine 110 / 410. If the transaction has been authorised, the POS machine 110 / 410 proceeds to complete the transaction, e.g., by displaying a notification message on a screen of the POS machine 110 / 410, and/or printing a transaction receipt for the user. If the transaction has been rejected by the issuer server 560, the POS machine 110 / 410 rejects the payment and displaying a transaction failure messaging, indicating that the transaction has been rejected.

[0074] Although the payment network shown in FIG. 5 includes the acquirer server 520, the payment network server 540 and the issuer sever 560, in some other embodiments, the POS machine 110 / 410 may be in communication with the issuer sever 560 directly, e.g., via one or more communication network.

[0075] A detailed example of a working flow for authorising transactions is illustrated in FIG. 6.

[0076] As shown in FIG. 6, at step 610, the user initiates a transaction at a POS machine using a card or a mobile computing device.

[0077] Accordingly, the transaction is initiated at the POS machine at step 620.

[0078] Next, at step 630, the Bluetooth address of the companion device, stored in the card or the mobile computing device, is sent to the POS machine.

[0079] Using the Bluetooth address of the companion device, the POS establishes a Bluetooth connection to the companion device at step 640. In some embodiments, the companion device is the mobile computing device using on which the mobile payment application is installed and executed. In some other embodiments, the companion device is a different electronic device from the mobile computing device on which the mobile payment application is installed and executed.

[0080] Next, at step 650, the companion device invokes a biometric authentication for authenticating the identity of the user, by capturing biometric characteristic(s) of the user, and comparing the captured biometric characteristic(s) with the biometric characteristic(s)

included in a biometric template stored in the companion device 130. The biometric characteristic may be one or more of the following: fingerprint, iris, voice and face.

[0081] At step 660, the companion device sends the biometric authentication results back to the POS machine.

[0082] At step 670, the POS machine sends a transaction request to an issuer associated with the financial account used by the user for making the payment, e.g., by sending a transaction request directly to an issuer server, or through a payment network as shown in FIG. 5.

[0083] At step 680, the issuer server returns an authorisation result indicating whether the transaction request is accepted or declined. The authorisation result may be determined by the issuer server at least in part based on the result of biometric authentication performed on the companion device.

[0084] Based on the authorisation result received form the issuer server, at step 690, the POS machine displays an outcome of the transaction, and may print out a receipt for the user if the transaction is successful.

[0085] According to at least some embodiments described hereinbefore, there is provided a method and system for authorising transactions using biometric authentication techniques. In the provided method and system, authentication of biometric features of the user is performed on the companion device rather than the electronic transaction device (e.g., a POS machine), with the result sent back to the transaction device, e.g., via Bluetooth or other wireless connections like NFC, WiFi, Zigbee, and so forth. In this way, the biometric template of the user does not need to be transmitted to or stored on the electronic transaction device, which may effectively enhancing the security of the transaction authorisation process.

[0086] Although the electronic transaction device in the embodiments described hereinbefore takes the form of a point-of-sale (POS) machine, it may alternatively be an automated teller machine (ATM), an automated ticket machine, or any other suitable device.

[0087] An example of the POS machine 110 / 410 shown in FIG. 1 and FIG. 4 is illustrated in FIG. 7.

[0088] The POS machine 110 / 410 includes at least one microprocessor 701, a memory 702, and an external input/output interface 703, interconnected via a bus 704. In some examples, the POS machine 110 / 410 may additionally include an input/output device 705, such as a PIN pad, and/or a display. In this example, the external interface 703 can connect the POS machine 110 / 410 to peripheral devices and/or networks, such as the mobile computing device 130 / 430, the payment network 140 /440, and/or additional local or remote storage devices. Although a single external interface 703 is shown, this is for the purpose of example only, and in practice multiple interfaces using different communication protocols (e.g. Ethernet, serial, USB, or wireless) may be provided. The POS machine 110 / 410 further includes a card reader or a NFC module 706 for communicating with the financial card or the mobile computing device 130 / 430, and a Bluetooth module 707 for communication via Bluetooth with the companion device, which may be the mobile computing device 130 / 430.

[0089] In use, the micro processor 701 executes machine-readable instructions stored in the memory 702 to perform the method described herein, including communicating with the the financial card or the mobile computing device 130 / 430, and the payment network 140 /440, as well as other process for authenticating transactions as described hereinbefore. The machine-readable instructions may include one or more software modules, and may be executed in a suitable execution environment, such as an operating system environment.

[0090] An example of the mobile computing device 130 / 430 shown in FIG. 1 and FIG. 4 is illustrated in FIG. 8.

[0091] The mobile computing device 130 / 430 includes at least one microprocessor 801, a memory 802, an input/output device 803 - such as a keyboard and/or display, or a touch screen - and an external input/output interface 804, interconnected via a bus 805. In this example, the external interface 804 can connect the mobile computing device 130 / 430 to peripheral devices and/or networks, such as the POS machine 110 / 410, and/or additional local or remote data store devices. Although a single external interface 804 is shown, this is for the purpose of example only, and in practice multiple interfaces using different communication protocols (e.g. Ethernet, serial, USB, or wireless) may be provided. The mobile computing device 130 / 430 further includes a NFC module 806 for communicating

with the POS machine 110 / 410, a Bluetooth module 807 for communication via Bluetooth with the POS machine 110 / 410, and a biometric authentication module 808 for capturing biometric characteristic(s) of the user for biometric authentication. The biometric authentication module 808 may be, for example, a fingerprint scanner, or a digital camera for capturing one or more images of the user's face.

[0092] In use, the microprocessor 801 executes machine-readable instructions stored in the memory 802 to allow the mobile computing device 130 / 430 to perform biometric authentication functions using the biometric authentication module 808, and to communicate with the POS machine 110 / 410, for example to initiate a transaction or to establish a Bluetooth connection with the POS machine 110 / 410. The machine-readable instructions may include one or more software modules, and may be executed in a suitable execution environment, such as a mobile operating system environment.

[0093] Throughout this specification and claims which follow, unless the context requires otherwise, the word "comprise", and variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated integer or group of integers or steps but not the exclusion of any other integer or group of integers.

[0094] Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A transaction device configured for processing transactions, the device including at least one processor configured to:

receive, from a payment device, one or more payment credentials and at least one device address of a companion device associated with the payment device, wherein the payment device is a payment card, wherein the companion device is a mobile device;

establish, a wireless connection with the companion device using the at least one device address;

receive, via the wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication; and

process a transaction request based on the one or more payment credentials and the biometric authentication result.

2. The device of claim 1, being configured to receive the device address from any one of: the companion device, a server in communication with the companion device, a payment application executable on the payment device or a payment card.

3. The device of any of claims claim 1 to 2, being configured to process the transaction request by sending the transaction request to a payment network when the biometric authentication result is positive.

4. The device of any of claims 1 to 3, the at least one processing device further configured to:

authenticate the companion device when the wireless connection is established.

5. The device of any of claims 1 to 4, wherein the biometric authentication result indicates verification of one or more of the following biometric characteristics of the user: fingerprint, iris, voice print and facial recognition.

6. The device of any of claims 1 to 5, wherein the at least one device address is associated with one payment device or companion device.

7. The device of any of claims 1 to 5, wherein the at least one device address is associated with multiple payment devices or companion devices.

8. A data-processor implemented method for processing transactions for a transaction device, the method including the steps of:

receiving, from a payment device, one or more payment credentials and at least one device address of a companion device associated with the payment device, wherein the payment device is a payment card, wherein the companion device is a mobile device;

establishing, a wireless connection with the companion device using the at least one device address;

receiving, via the wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication; and

processing a transaction request based on the one or more payment credentials and the biometric authentication result.

9. A non-transitory computer readable storage medium embodying thereon a program of computer readable instructions which, when executed by one or more processors of a POS device in communication with at least one companion device, cause the POS device to carry out a method for processing transactions, the method embodying the steps of:

receiving, from a payment device, one or more payment credentials and at least one device address of a companion device associated with the payment device, wherein the payment device is a payment card, wherein the companion device is a mobile device;

establishing, a wireless connection with the companion device using the at least one device address;

receiving, via the wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication; and

processing a transaction request based on the one or more payment credentials and the biometric authentication result.

10. A payment device configured for processing transactions, the device including at least one processor configured to:

transmit, to a transaction device for processing transactions, one or more payment credentials and at least one device address of a companion device associated with the payment device, wherein the payment device is a payment card, wherein the companion device is a mobile device; and

transmit, to a transaction device for processing transactions, via a wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication.

11. The device of claim 10, wherein the biometric authentication result indicates verification of one or more of the following biometric characteristics of the user: fingerprint, iris, voice print and facial recognition.

12. The device of either claim 10 or 11, wherein the at least one device address is associated with one payment device or companion device.

13. The device of either claim 10 or 11, wherein the at least one device address is associated with multiple payment devices or companion devices.

14. A data-processor implemented method for processing transactions, the method including the steps of:

transmitting, to a transaction device for processing transactions, one or more payment credentials and at least one device address of a companion device associated with the payment device, wherein the payment device is a payment card, wherein the companion device is a mobile device; and

transmitting, to the transaction device for processing transactions, via a wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication.

15. A non-transitory computer readable storage medium embodying thereon a program of computer readable instructions which, when executed by one or more processors of a payment device in communication with at least one companion device, cause the payment device to carry out a method for processing transactions, wherein the payment device is a payment card, wherein the companion device is a mobile device, the method embodying the steps of:

transmitting, to a transaction device for processing transactions, one or more payment credentials and at least one device address of a companion device associated with the payment device; and

transmitting, to the transaction device for processing transactions, via a wireless connection, a biometric authentication result from a sensor of the companion device, the biometric authentication result representing a result of verifying a user's identity by biometric authentication.