

CONTACTLESS DELIVERY SYSTEMS AND METHODS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Patent Application No. 17/160,049 filed January 27, 2021, the disclosure of which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

[0002] The present disclosure relates generally to delivery management, and more particularly, to contactless delivery systems and methods.

BACKGROUND

[0003] Electronic commerce is becoming increasingly widespread and common. Online shopping, where items are purchased online and shipped to the purchasing customer at a residential address, commercial address, or other location, constitutes a large and growing sector of the global economy. With the number and value of goods purchased online and shipped for delivery increasing, along in-store pickup and other forms of receiving goods, it is critical that efficient, timely, and secure deliveries can be made.

[0004] In social distancing scenarios, it is difficult to identify people without close physical personal contact. For example, when a package is delivered to a customer, the customer generally needs to identify himself or herself to complete the delivery and receive the package. As another example, a customer may arrange to pick up a package from a store, and the customer may call a phone number indicating he or she has arrived at the store. But the customer has to identify himself or herself to ensure the secure pick up of the package, and presenting a form of identification (e.g., a driver's license) to store personnel is difficult without physical contact or coming into close proximity to store personnel. In another example, a package may be delivered to a customer by a delivery person, and this may

require the customer to verify himself or herself to the delivery person, such that the package can be delivered to the correct recipient and in a secure manner. In many such interactions, social distancing is not possible and the identification and verification process is not efficient.

[0005] These and other deficiencies exist. Accordingly, there is a need to provide systems and methods that overcome these deficiencies to verify customers in a secure and efficient manner while minimizing physical contact or close interactions between people.

SUMMARY

[0006] Aspects of the disclosed technology include systems and methods for contactless package delivery.

[0007] Embodiments of the present disclosure provide a contactless delivery system. The contactless delivery system includes a contactless card. The contactless card includes a processor and a memory. The memory stores a cryptogram that contains a unique identifier associated with a user account. After entry into a communication field, the contactless card is configured to transmit the cryptogram to a server via one or more intermediary devices. Upon receipt of the cryptogram, the server is configured to: validate the cryptogram; decrypt the cryptogram and extract the unique identifier; query, using the unique identifier, a database for an identity of the user account; generate a digital signature based on the identity of the user account; and transmit a verification notification including the identity of the user account and the digital signature.

[0008] Embodiments of the present disclosure provide a contactless delivery system. The contactless system includes a server comprising a processor and a memory. The server is configured to: receive a cryptogram containing an unique identifier associated with a user account; validate the cryptogram; decrypt the cryptogram and extract the unique identifier;

query, using the unique identifier, a database for an identity of the user account; generate a digital signature based on the identity of the user account; and transmit a verification notification including the identity of the user account and the digital signature.

[0009] Embodiments of the present disclosure provide a contactless delivery method. The contactless method comprises: receiving a cryptogram, the cryptogram containing an unique identifier associated with a user account; validating the cryptogram; decrypting the cryptogram and extracting the unique identifier; querying, using the unique identifier, a database for an identity of the user account; generating a digital signature based on the identity of the user account; and transmitting a verification notification including the identity of the user account and the digital signature.

[0010] Further features of the disclosed systems and methods, and the advantages offered thereby, are explained in greater detail hereinafter with reference to specific example embodiments illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Figure 1 is a diagram of a system for contactless delivery according to an example embodiment.

[0012] Figure 2 is a sequence chart illustrating a method of contactless delivery according to an example embodiment.

[0013] Figure 3 is a flow chart illustrating a method of contactless delivery according to an example embodiment.

[0014] Figure 4 is a flow chart illustrating a method of contactless delivery according to an example embodiment.

[0015] Figures 5 is a diagram of a system for contactless delivery according to an example

embodiment.

[0016] Figure 6 is a sequence chart illustrating a method of contactless delivery according to an example embodiment.

[0017] Figure 7 is a flow chart illustrating a method of contactless delivery according to an example embodiment.

[0018] Figure 8 is a flow chart illustrating a method of contactless delivery according to an example embodiment.

[0019] Figure 9 is a flow chart illustrating a method of contactless delivery according to an example embodiment.

[0020] Figure 10 is a flow chart illustrating a method of contactless delivery according to an example embodiment.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

[0021] The following description of embodiments provides non-limiting representative examples referencing numerals to particularly describe features and teachings of different aspects of the invention. The embodiments described should be recognized as capable of implementation separately, or in combination, with other embodiments from the description of the embodiments. A person of ordinary skill in the art reviewing the description of embodiments should be able to learn and understand the different described aspects of the invention. The description of embodiments should facilitate understanding of the invention to such an extent that other implementations, not specifically covered but within the knowledge of a person of skill in the art having read the description of embodiments, would be understood to be consistent with an application of the invention.

[0022] Many consumers and merchants are seeking to complete transactions efficiently, and

also seeking to complete transactions in a socially distant manner where employees or other personnel do not have to come into close physical proximity with consumers. This is particularly true during times when many people are concern about spreading germs, such as during a pandemic, and accordingly new ways are needed to interact and complete transactions without bringing people into close proximity with each other. This can be difficult because people depend heavily on physical evidence of identity (e.g., driver license, physical signature, birth certificate, passport, etc.) to verify their identity. Moreover, common forms of identification, such as photographic identification and physical signatures, may be outdated, may not be reliable, and may not even be particularly meaningful. In such cases, digital ways may be needed, for example, to sign for packages, show driver license for purchases, and produce car registration for an officer.

[0023] Example embodiments of the present disclosure provide systems and methods for contactless delivery. The disclosed system and method may also be used beyond the contactless package delivery, such as in a pandemic time in terms of maintaining safety for people. A contactless card or other device may be tapped to a device (e.g., a smart phone) to exchange identities at a distance. Accordingly, a delivery person can verify that they are delivering a package to the right person, and the person accepting the package can also verify that the delivery person who is delivering to them is authorized to make the delivery. In some embodiments, certified immunity documents of both the person accepting the package and the delivery person may be used to understand about the person's immunity or a company's policies around sanitation.

[0024] In some embodiments, when a contactless card or other device is tapped to a person's phone, certificates signed by an employer (e.g., a courier) can also be transferred. This transfer

can be either directly from the contactless card, the person's phone, or indirectly after looking up their identity online.

[0025] In some embodiments, when a contactless card is tapped to a package delivery device, the identity of the person who taps the contactless card can be determined and verified to match the addressee of the package. This can also be implemented with host card emulation (HCE) that emulates the contactless card. The address on the package may be a loose address (stored preferences) or tight with digitally signed certificates, or may be scoped to the individual delivery transaction.

[0026] Example embodiments of the present disclosure can promote the efficiency and security of transactions, such as package pickup and delivery transactions and the purchase of goods or services subject to age restrictions, quantity restrictions, and other restrictions. In addition, the identity verification can be carried out without the need for consumers and employees or other personnel to come within close proximity to each other. Further, the identity verification can be carried out quickly, without degrading the user experience and without the need for consumers, employees, and other personnel to carry identification documents and other materials. It is understood that example embodiments of the present disclosure are applicable to a wide range of purposes where identity verification is required, including, without limitation, package pickup, package delivery, security (e.g., building or restricted area access), and travel (e.g., ticket purchases, plane or train boarding).

[0027] Figure 1 illustrates a system 100 for contactless package delivery according to an example embodiment. As further discussed below, the system 100 may include a contactless card 110, a delivery device 120, a server 130, and a database 140 in communication using a network 150. Although Figure 1 illustrates single instances of the components, the system 100

may include any number of components.

[0028] The contactless card 110 can be configured to transmit a cryptogram to the delivery device 120 upon tapping to the delivery device 120. The delivery device 120 may be configured to read the cryptogram from the contactless card 110 after entry of the contactless card 110 into a communication field of the delivery device 120. The delivery device 120 may then transmit the cryptogram to the server 130. The server 130 may be configured to verify the cryptogram by searching the database 140.

[0029] The contactless card 110 can perform authentication and numerous other functions that may otherwise require a user to carry a separate physical token in addition to the contactless card 110. By employing a contactless interface, the contactless card 110 may be provided with a method to interact and communicate between a user's device (such as a mobile phone or the delivery device 120) and the card itself. For example, the Europay, Mastercard, and Visa (EMV) protocol, which underlies many credit card transactions, includes an authentication process which suffices for operating systems for Android® but presents challenges for iOS®, which is more restrictive regarding near field communication (NFC) usage, as it can be used only in a read-only manner. Exemplary embodiments of the contactless card 110 described herein utilize NFC technology.

[0030] The contactless card 110, which may comprise a payment card, such as a credit card, debit card, or gift card, may be issued by a service provider displayed on the front or back of the contactless card 110. In some examples, the contactless card 110 is not related to a payment card, and may comprise, without limitation, an identification card, a membership card, and a travel card. In some examples, the contactless card 110 may comprise a dual interface contactless payment card. The contactless card 110 may comprise a substrate, which may

include a single layer or one or more laminated layers composed of plastics, metals, and other materials. Exemplary substrate materials include polyvinyl chloride, polyvinyl chloride acetate, acrylonitrile butadiene styrene, polycarbonate, polyesters, anodized titanium, palladium, gold, carbon, paper, and biodegradable materials. In some examples, the contactless card 110 may have physical characteristics compliant with the ID-1 format of the ISO/IEC 7810 standard, and the contactless card 110 may otherwise be compliant with the ISO/IEC 14443 standard. However, it is understood that the contactless card 110 according to the present disclosure may have different characteristics, and the present disclosure does not require the contactless card 110 to be implemented in a payment card.

[0031] The contactless card 110 may also include identification information displayed on the front and/or back of the contactless card 110, and a contact pad. The contact pad may be configured to establish contact with another communication device, such as a user device, smart phone, laptop, desktop, or tablet computer. The contactless card 110 may also include processing circuitry, antenna and other components. These components may be located behind the contact pad or elsewhere on the substrate. The contactless card 110 may also include a magnetic strip or tape, which may be located on the back of the contactless card 110.

[0032] The contact pad of the contactless card 110 may include processing circuitry for storing and processing information, including a processor 111 and a memory 112. It is understood that the processing circuitry may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein.

[0033] The memory 112 may be a read-only memory, write-once read-multiple memory or

read/write memory, e.g., RAM, ROM, and EEPROM, and the contactless card 110 may include one or more of these memories. A read-only memory may be factory programmable as read-only or one-time programmable. One-time programmability provides the opportunity to write once then read many times. A write once/read-multiple memory may be programmed at a point in time after the memory chip has left the factory. Once the memory is programmed, it may not be rewritten, but it may be read many times. A read/write memory may be programmed and re-programmed many times after leaving the factory. It may also be read many times.

[0034] The memory 112 may be configured to store one or more applets 113, one or more counters 114, and a unique customer identifier 115. The one or more applets 113 may comprise one or more software applications configured to execute on one or more contactless cards, such as Java Card applet. However, it is understood that the one or more applets 113 are not limited to Java Card applets, and instead may be any software application operable on contactless cards or other devices having limited memory. The one or more counters 114 may comprise a numeric counter sufficient to store an integer. The unique customer identifier 115 may comprise a unique alphanumeric identifier assigned to a user of the contactless card 110, and the identifier may distinguish the user of the contactless card 110 from other contactless card users. In some examples, the customer identifier 115 may identify both a customer and an account assigned to that customer and may further identify the contactless card 110 associated with the customer's account.

[0035] The processor 111 and memory 112 elements of the foregoing exemplary embodiments are described with reference to the contact pad, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the contact pad or entirely

separate from it, or as further elements in addition to the processor 111 and the memory 112 elements located within the contact pad.

[0036] In some examples, the contactless card 110 may comprise one or more antennas. The one or more antennas may be placed within the contactless card 110 and around the processing circuitry of the contact pad. For example, the one or more antennas may be integral with the processing circuitry and the one or more antennas may be used with an external booster coil. As another example, the one or more antennas may be external to the contact pad and the processing circuitry.

[0037] In an embodiment, the coil of contactless card 110 may act as the secondary of an air core transformer. A terminal may communicate with the contactless card 110 by cutting power or amplitude modulation. The contactless card 110 may infer the data transmitted from the terminal using the gaps in the contactless card's power connection, which may be functionally maintained through one or more capacitors. The contactless card 110 may communicate back by switching a load on the contactless card's coil or load modulation. Load modulation may be detected in the terminal's coil through interference.

[0038] As explained above, the contactless card 110 may be built on a software platform operable on smart cards or other devices having limited memory, such as JavaCard, and one or more or more applications or applets may be securely executed. Applets may be added to contactless cards to provide a one-time password (OTP) for multifactor authentication (MFA) in various mobile application-based use cases. Applets may be configured to respond to one or more requests, such as near field data exchange requests, from a reader, such as a mobile NFC reader, and produce an NDEF message that comprises a cryptographically secure OTP encoded as an NDEF text tag.

[0039] The delivery device 120 may be a network-enabled computer device. Exemplary network-enabled computer devices include, without limitation, a server, a network appliance, a personal computer, a workstation, a phone, a handheld personal computer, a personal digital assistant, a thin client, a fat client, an Internet browser, a mobile device, a kiosk, a contactless card, or other a computer device or communications device. For example, network-enabled computer devices may include an iPhone, iPod, iPad from Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[0040] The delivery device 120 may include a processor 121, a memory 122, and an application 123. The processor 121 may be a processor, a microprocessor, or other processor, and the delivery device 120 may include one or more of these processors. The processor 121 may include processing circuitry, which may contain additional components, including additional processors, memories, error and parity/CRC checkers, data encoders, anti-collision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein.

[0041] The processor 121 may be coupled to the memory 122. The memory 122 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the delivery device 120 may include one or more of these memories. A read-only memory may be factory programmable as read-only or one-time programmable. One-time programmability provides the opportunity to write once then read many times. A write-once read-multiple memory may be programmed at a point in time after the memory chip has left the factory. Once the memory is programmed, it may not be rewritten, but it may be

read many times. A read/write memory may be programmed and re-programmed many times after leaving the factory. It may also be read many times. The memory 122 may be configured to store one or more software applications, such as the application 123, and other data, such as user's shopping and financial account information.

[0042] The application 123 may comprise one or more software applications, such as a package delivery application and a contactless card reading application, comprising instructions for execution on the delivery device 120. In some examples, the delivery device 120 may execute one or more applications, such as software applications, that enable, for example, network communications with one or more components of the system 100, transmit and/or receive data, and perform the functions described herein. Upon execution by the processor 121, the application 123 may provide the functions described in this specification, specifically to execute and perform the steps and functions in the process flows described below. For example, the package delivery application of the application 123 may be executed to perform retrieving information of a package delivery stored in the database 140; the contactless card reading application of the application 123 may be executed to perform communications with the contactless card 110. Such processes may be implemented in software, such as software modules, for execution by computers or other machines. The application 123 may provide GUIs through which a user may view and interact with other components and devices within the system 100. The GUIs may be formatted, for example, as web pages in HyperText Markup Language (HTML), Extensible Markup Language (XML) or in any other suitable form for presentation on a display device depending upon applications used by users to interact with the system 100.

[0043] The delivery device 120 may further include a display 124 and input devices 125. The

display 124 may be any type of device for presenting visual information such as a computer monitor, a flat panel display, and a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays. The input devices 125 may include any device for entering information into the delivery device 120 that is available and supported by the delivery device 120, such as a touch-screen, keyboard, mouse, cursor-control device, touch-screen, microphone, digital camera, video recorder or camcorder. These devices may be used to enter information and interact with the software and other devices described herein. For example, the input devices 125 may comprise a card reader. The card reader may be configured to read from and/or communicate with the contactless card 110. In conjunction with the application 123, the card reader may communicate with the contactless card 110 using short-range wireless communication (e.g., NFC).

[0044] The server 130 may be a network-enabled computer device. Exemplary network-enabled computer devices include, without limitation, a server, a network appliance, a personal computer, a workstation, a phone, a handheld personal computer, a personal digital assistant, a thin client, a fat client, an Internet browser, a mobile device, a kiosk, a contactless card, or other a computer device or communications device. For example, network-enabled computer devices may include an iPhone, iPod, iPad from Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[0045] The server 130 may include a processor 131, a memory 132, and an application 133. The processor 131 may be a processor, a microprocessor, or other processor, and the server 130 may include one or more of these processors. The processor 131 may include processing

circuitry, which may contain additional components, including additional processors, memories, error and parity/CRC checkers, data encoders, anti-collision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein.

[0046] The processor 131 may be coupled to the memory 132. The memory 132 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the server 130 may include one or more of these memories. A read-only memory may be factory programmable as read-only or one-time programmable. One-time programmability provides the opportunity to write once then read many times. A write-once read-multiple memory may be programmed at a point in time after the memory chip has left the factory. Once the memory is programmed, it may not be rewritten, but it may be read many times. A read/write memory may be programmed and re-programmed many times after leaving the factory. It may also be read many times. The memory 132 may be configured to store one or more software applications, such as the application 133, and other data, such as user's shopping and financial account information.

[0047] The application 133 may comprise one or more software applications comprising instructions for execution on the server 130. In some examples, the server 130 may execute one or more applications, such as software applications, that enable, for example, network communications with one or more components of the system 100, transmit and/or receive data, and perform the functions described herein. Upon execution by the processor 131, the application 133 may provide the functions described in this specification, specifically to execute and perform the steps and functions in the process flows described below. For example, the application 133 may be executed to perform verifying a cryptogram. Such

processes may be implemented in software, such as software modules, for execution by computers or other machines. The application 133 may provide GUIs through which a user may view and interact with other components and devices within the system 100. The GUIs may be formatted, for example, as web pages in HyperText Markup Language (HTML), Extensible Markup Language (XML) or in any other suitable form for presentation on a display device depending upon applications used by users to interact with the system 100.

[0048] The server 130 may further include a display 134 and input devices 135. The display 134 may be any type of device for presenting visual information such as a computer monitor, a flat panel display, and a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays. The input devices 135 may include any device for entering information into the server 130 that is available and supported by the server 130, such as a touch-screen, keyboard, mouse, cursor-control device, touch-screen, microphone, digital camera, video recorder or camcorder. These devices may be used to enter information and interact with the software and other devices described herein.

[0049] The database 140 may be one or more databases configured to store data, including without limitation, private information of users, financial accounts of users, identities of users, transactions of users, and certified and uncertified documents. The database 140 may comprise a relational database, a non-relational database, or other database implementations, and any combination thereof, including a plurality of relational databases and non-relational databases. In some examples, the database 140 may comprise a desktop database, a mobile database, or an in-memory database. Further, the database 140 may be hosted internally by the server 130 or may be hosted externally of the server 130, such as by a server, by a cloud-based platform, or in any storage device that is in data communication with the server 130.

[0050] The system 100 may include one or more networks 150. In some examples, the network 150 may be one or more of a wireless network, a wired network or any combination of wireless network and wired network, and may be configured to connect the delivery device 120, the server 130, and the database 140. For example, the network 150 may include one or more of a fiber optics network, a passive optical network, a cable network, an Internet network, a satellite network, a wireless local area network (LAN), a Global System for Mobile Communication, a Personal Communication Service, a Personal Area Network, Wireless Application Protocol, Multimedia Messaging Service, Enhanced Messaging Service, Short Message Service, Time Division Multiplexing based systems, Code Division Multiple Access based systems, D-AMPS, Wi-Fi, Fixed Wireless Data, IEEE 802.11b, 802.15.1, 802.11n and 802.11g, Bluetooth, NFC, Radio Frequency Identification (RFID), Wi-Fi, and/or the like.

[0051] In addition, the network 150 may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 902.3, a wide area network, a wireless personal area network, a LAN, or a global network such as the Internet. In addition, the network 150 may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. The network 150 may further include one network, or any number of the exemplary types of networks mentioned above, operating as a stand-alone network or in cooperation with each other. The network 150 may utilize one or more protocols of one or more network elements to which they are communicatively coupled. The network 150 may translate to or from other protocols to one or more protocols of network devices. Although the network 150 is depicted as a single network, it should be appreciated that according to one or more examples, the network 150 may comprise a plurality of interconnected networks, such as, for example, the Internet, a service provider's network, a cable television network, corporate

networks, such as credit card association networks, and home networks. The network 150 may further comprise, or be configured to create, one or more front channels, which may be publicly accessible and through which communications may be observable, and one or more secured back channels, which may not be publicly accessible and through which communications may not be observable.

[0052] In some examples, communications between the delivery device 120, server 130, and the database 140 using the network 150 can occur using one or more front channels and one or more secure back channels. A front channel may be a communication protocol that employs a publicly accessible and/or unsecured communication channel such that a communication sent to the delivery device 120, server 130, and/or database 140 may originate from any other device, whether known or unknown to the delivery device 120, server 130, and/or database 140, if that device possesses the address (e.g., network address, Internet Protocol (IP) address) of the delivery device 120, server 130, and/or database 140. Exemplary front channels include, without limitation, the Internet, an open network, and other publicly-accessible communication networks. In some examples, communications sent using a front channel may be subject to unauthorized observation by another device. In some examples, front channel communications may comprise Hypertext Transfer Protocol (HTTP) secure socket layer (SSL) communications, HTTP Secure (HTTPS) communications, and browser-based communications with a server or other device.

[0053] A secure back channel may be a communication protocol that employs a secured and/or publicly inaccessible communication channel. A secure back channel communication sent to the delivery device 120, server 130, and/or database 140 may not originate from any device, and instead may only originate from a selective number of parties. In some examples, the

selective number of devices may comprise known, trusted, or otherwise previously authorized devices. Exemplary secure back channels include, without limitation, a closed network, a private network, a virtual private network, an offline private network, and other private communication networks. In some examples, communications sent using a secure back channel may not be subject to unauthorized observation by another device. In some examples, secure back channel communications may comprise Hypertext Transfer Protocol (HTTP) secure socket layer (SSL) communications, HTTP Secure (HTTPS) communications, and browser-based communications with a server or other device.

[0054] In some examples, the contactless card 110 may be associated with a user and can be used by that user, for example, a customer to whom a package is delivered. The delivery device 120 can be associated with a package delivery person and may be operated by that person, such as a delivery person of a courier. The server 130 can be associated with a financial institution, such as a bank or a credit card company that offers financial services to the user of the contactless card 110. The contactless card 110 may be issued by the financial institution. However, it is understood that the present disclosure encompasses any entities, and is not limited to financial institutions.

[0055] Figure 2 illustrates a sequence diagram 200 of contactless package delivery according to an example embodiment. Figure 2 may reference the same or similar components as those illustrated in Figure 1, including a contactless card, a delivery device, a server, a database, and a network.

[0056] In step 210, a contactless card (e.g., the contactless card 110) transmits a cryptogram after entry of the contactless card into a communication field of a delivery device (e.g., the delivery device 120). The contactless card may be tapped by a user to the delivery device.

The delivery device may be configured to have a card reader to read a cryptogram from the contactless card upon the tap. The card reader may comprise a communication interface to generate a communication field of the card reader. As used herein, a tap of the contactless card to the delivery device may not indicate that the contactless card is in a physical contact with the delivery device. A tap of the contactless card to the delivery device may refer to entry of the contactless card into the communication field of the card reader. The cryptogram may be stored in a memory of the contactless card. The cryptogram may be associated with a unique identifier of a user account.

[0057] In step 215, the delivery device may transmit the cryptogram to a server (e.g., the server 130). Upon reading the cryptogram from the contactless card, the delivery device transmits the cryptogram to the server via a network (e.g., the network 150). Prior to transmission, the cryptogram may be encrypted by the contactless card.

[0058] In step 220, the server validates the cryptogram, decrypts the cryptogram and extracts the unique identifier. When the server receives the cryptogram, the server may decrypt the cryptogram after verifying the cryptogram. The server may then extract the unique identifier of the user account.

[0059] In step 225, the server 130 may query, using the unique identifier, for an identity of the user account. In this step, the server communicates with a database (e.g., the database 140) for searching for the identity of the user account. The identity of the user account is stored on the database. The identity of the user account may comprise a name of the user who taps the contactless card. The user account may comprise one or more email addresses associated with the user, a phone number of the user, a mailing address of the user, and so forth. Once the

identity of the user account matches the unique identifier of the user account, the user of the contactless card is verified.

[0060] In step 230, the server may generate a digital signature based on the identity of the user account. After obtaining and verifying the identity of the user account, the server may be configured to generate a digital signature of the identity. The digital signature may be a signature of the user name or other signatures associated with the user name.

[0061] In step 235, the server may transmit a verification notification including the identity of the user account and the digital signature to the delivery device. The verification notification may indicate that the user of the contactless card has been verified, what the identity of the user is, and the digital signature of the identity.

[0062] When the delivery device receives the verification notification, the delivery device may display the verification notification on the display of the delivery device. The delivery device may be configured to sign a package receipt document using the digital signature.

[0063] Figure 3 illustrates a flow chart for a method 300 of contactless package delivery according to an example embodiment. Figure 3 may reference the same or similar components as those illustrated in Figure 1 and Figure 2, including a contactless card, a delivery device, a server, a database, and a network. The method 300 may be implemented in the system 100 and may comprise the following steps.

[0064] In step 305, a contactless card transmits a cryptogram to a server via one or more intermediary device. As used herein, the contactless card, which may comprise a payment card, such as a credit card, debit card, or gift card, issued by a service provider displayed on the front or back of the contactless card. In some examples, the contactless card is not related to a payment card, and may comprise, without limitation, an identification card. In some

examples, the payment card may comprise a dual interface contactless payment card. The contactless card may store the cryptogram in its memory and transmit the cryptogram to the server upon being tapped to the one or more intermediary device. The one or more intermediary device may comprise a delivery device (e.g., the delivery device 120).

[0065] The cryptogram may contain a unique identifier associated with a user/customer account. The cryptogram may further contain a counter value and a plurality of keys, and the processor of the contactless card is configured to generate the cryptogram using the counter value, the plurality of keys, and the unique identifier.

[0066] The counter value may be updated by the contactless card with every conversation between the contactless card and the one or more intermediary device.

[0067] For example, the contactless card communicates with the one or more intermediary device after being brought near the contactless card. Communication between the one or more intermediary device and the contactless card may involve the contactless card being sufficiently close to a card reader of the one or more intermediary device to enable near field communication (NFC) data transfer between the one or more intermediary device and the contactless card.

[0068] In other embodiments, the contactless card may communicate with the intermediary device through other means including, but not limited to, Bluetooth, satellite, Wi-Fi, wired communications, and/or any combination of wireless and wired connections. According to some embodiments, the contactless card may be configured to communicate with the card reader of the intermediary device through NFC when the contactless card is within range of card reader. In other examples, communications with the contactless card may be

accomplished through a physical interface, e.g., a universal serial bus interface or a card swipe interface.

[0069] In step 310, the server validates the cryptogram. In some examples, the cryptogram may be a message authentication code (MAC) cryptogram. The MAC cryptogram may be created from a message including a shared secret. The server may generate an additional MAC cryptogram based on the shared secret, and compare the additional MAC cryptogram with the MAC cryptogram received from the contactless card. If the additional MAC cryptogram matches with the MAC cryptogram received from the contactless card, the MAC cryptogram received from the contactless card is validated.

[0070] In some embodiments, each time the contactless card is read, the counter value is transmitted to the server. This may be done in order to determine whether the counter value is equal to a counter value maintained by the server for validation and security purposes. The one or more counters may be configured to prevent a replay attack. For example, if the cryptogram has been obtained and replayed, that cryptogram is immediately rejected if the counter has been read or used or otherwise passed over. If the counter has not been used, it may be replayed. In some examples, the counter value that is updated on the contactless card is different from the counter that is updated for transactions. In some examples, the contactless card may comprise a first applet, which may be a transaction applet, and a second applet. Each applet may comprise a counter.

[0071] In some examples, the counter may get out of sync between the contactless card and the server. For example, the contactless card may be activated causing the counter to be updated and a new communication to be generated by the contactless card, but the communication may be not be transmitted for processing at the server. This may cause the

counter of the contactless card and the counter maintained at the server to get out of sync. This may occur unintentionally including, for example, where a contactless card is stored adjacent to a device (e.g., carried in a pocket with a device) and where the contactless card is read at an angle may include the card being misaligned or not positioned such that the contactless card is powered up in the NFC field but is not readable. If the contactless card is positioned adjacent to a device, the device's NFC field may be turned on to power the contactless card causing the counter therein to be updated, but no application on the device receives the communication.

[0072] To keep the counter in sync, an application, such as a background application, may be executed that would be configured to detect when the intermediary device wakes up and synchronize with the server indicating that a read that occurred due to detection to then move the counter forward. Since the counters of the contactless card and the server may get out of sync, the server may be configured to allow the counter of the contactless card to be updated a threshold or predetermined number of times before it is read by the server and still be considered valid. For example, if the counter is configured to increment (or decrement) by one for each occurrence indicating activation of the contactless card, the server may allow any counter value it reads from the contactless card as valid, or any counter value within a threshold range (e.g., from 1 to 10). Moreover, the server may be configured to request a gesture associated with the contactless card, such as a user tap, if it reads a counter value which has advanced beyond 10, but below another threshold range value (such as 1000). From the user tap, if the counter value is within a desired or acceptance range, authentication succeeds.

[0073] In step 315, the server decrypts the cryptogram. The cryptogram may be encrypted by the contactless card prior to transmission to the server. The cryptogram may be encrypted using one or more cryptographic algorithms which may comprise at least one of a symmetric

encryption algorithm, a hash-based message authentication code (HMAC) algorithm, and a cipher-based message authentication code (CMAC) algorithm. The server may decrypt the cryptogram using the one or more cryptographic algorithms.

[0074] In step 320, the server extracts the unique identifier from the decrypted cryptogram. The unique identifier may comprise a unique alphanumeric identifier assigned to a user of the contactless card. The unique identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the unique identifier may identify both a customer and an account assigned to that customer and may further identify the contactless card associated with the customer's account.

[0075] In step 325, the server queries, using the unique identifier, a database for an identity of the user account. In some embodiments, the unique identifier that is cryptographically secure and not susceptible to interception may be transmitted to one or more backend services. The unique identifier may be configured to look up secondary information about individual. The secondary information may comprise personally identifiable information about the user (e.g., an identity of the user). In some examples, the secondary information may be stored within the contactless card.

[0076] In step 330, the server generates a digital signature based on the identity of the user account. After verifying and retrieving the identity of the user account, the server may generate a digital signature of the user using the identity. The identity of the user may be the name of the user. The digital signature can a signature in any suitable form.

[0077] In step 335, the server transmits a verification notification including the identity of the user account and the digital signature to the delivery device. The verification notification may indicate that the user/customer who tapped the contactless card to the delivery device has been

verified. When receiving the verification notification, the delivery device may display the verification notification on a display of the delivery device. The delivery device may display the digital signature next to the user/customer name to whom the package is delivered. This digital signature may be considered as an authorization and verification for releasing the package to the user.

[0078] Figure 4 illustrates a flow chart for a method 400 of contactless package delivery according to an example embodiment. Figure 4 may reference the same or similar components as those illustrated in Figures 1-3, including a contactless card, a delivery device, a server, a database, and a network. The method 400 may comprise the following steps.

[0079] In some embodiments, one or more authentication factors may be used to verify an identity of the user in addition to the unique identifier of the user account. The one or more authentication factors may be any suitable factors as described below.

[0080] In step 405, a contactless card transmits a cryptogram to a server via one or more intermediary devices. The contactless card may store the cryptogram in its memory and transmit the cryptogram to the server upon being tapped to the one or more intermediary device. The cryptogram may contain a unique identifier associated with a user/customer account. The one or more intermediary device may comprise a delivery device (e.g., the delivery device 120).

[0081] In step 410, the server validates the cryptogram. The cryptogram may be a MAC cryptogram. The MAC cryptogram may be created from a message including a shared secret. The server may generate an additional MAC cryptogram based on the shared secret, and compare the additional MAC cryptogram with the MAC cryptogram received from the contactless card. If the additional MAC cryptogram matches with the MAC cryptogram

received from the contactless card, the MAC cryptogram received from the contactless card is validated.

[0082] In step 415, the server decrypts the cryptogram. The cryptogram may be encrypted using one or more cryptographic algorithms prior to transmission to the server. The server may decrypt the cryptogram using the one or more cryptographic algorithms.

[0083] In step 420, the server extracts the unique identifier. The unique identifier may be used to distinguish the user of the contactless card from other contactless card users. The unique identifier may identify both a customer and an account assigned to that customer and may further identify the contactless card associated with the customer's account.

[0084] In step 425, the server queries, using the unique identifier, a database for an identity of the user account. The unique identifier may be configured to look up secondary information about an individual. The secondary information may comprise personally identifiable information about the user (e.g., an identity of the user).

[0085] In step 430, the server receives from the database, one or more documents to verify the identity of the user account. The one or more documents may be stored in the database. In other embodiments, the one or more documents may be stored in the contactless card and are transmitted to the server when the contactless card is read by the intermediary device (e.g., the delivery device). In other embodiments, the one or more documents may be stored in the delivery device and are transmitted to the server along with the cryptogram when the contactless card is read by the delivery device.

[0086] The one or more documents may be certified documents, such as certificates signed by an employer (e.g., a courier). The one or more documents may also include information on a delivery package stored on the delivery device, which may be transmitted to the server by the

delivery device as an authentication factor for verifying the identity of the user. The information on the delivery package may include the name of the user, a delivery address of the user, a phone number of the user, and so forth. The one or more documents may also be uncertified documents such as a copy of a driver license of the user. In some embodiments, the one or more documents may include a profile picture of the user account, which can be transmitted to the server for verifying the identity of the user account.

[0087] In step 435, the server generates a digital signature based on the identity of the user account. The identity of the user may be the name of the user. The digital signature can a signature in any suitable form.

[0088] In step 440, the server transmits a verification notification including the identity of the user account and the digital signature. When receiving the verification notification, the delivery device may display the digital signature next to the user/customer name to whom the package is delivered. This digital signature may be considered as an authorization and verification for releasing the package to the user.

[0089] Unlike the system 100 in Figure 1, in some embodiments, the intermediary device may be a user device other than the delivery device. The contactless card may be tapped to the user device that transmits the cryptogram to the server. The delivery device can receive the verification notification. Figure 5 illustrates such a system 500 of contactless package delivery according to an example embodiment. As further discussed below, the system 500 may include a contactless card 510, a user device 520, a server 530, a database 540, and a delivery device 550 in communication using a network 560. Although Figure 5 illustrates single instances of the components, the system 500 may include any number of components.

[0090] The contactless card 510 can be configured to transmit a cryptogram to the user device 520 upon tapping to the user device 520. The user device 520 may be configured to read the cryptogram from the contactless card 510 after entry of the contactless card 510 into a communication field of the user device 520. The user device 520 may then transmit the cryptogram to the server 530. The server 530 may be configured to verify the cryptogram by searching the database 540. The server 530 may transmit a verification notification including a digital signature to the delivery device 550.

[0091] The contactless card 510 can include processing circuitry for storing and processing information, including a microprocessor 511 and a memory 512. The memory 512 may be configured to store one or more applets 513, one or more counters 514, and a unique customer identifier 515. In some examples, the contactless card 510 is similar to the contactless card 110 in Figure 1.

[0092] The user device 520 may be a network-enabled computer device. The user device 520 may include a processor 521, a memory 522, and an application 523. The application 523 may comprise one or more software applications, such as a contactless card reading application, comprising instructions for execution on the user device 520. The user device 520 may further include a display 524 and input devices 525.

[0093] The user device 520 may be a network-enabled computer device. Exemplary network-enabled computer devices include, without limitation, a server, a network appliance, a personal computer, a workstation, a phone, a handheld personal computer, a personal digital assistant, a thin client, a fat client, an Internet browser, a mobile device, a kiosk, a contactless card, or other a computer device or communications device. For example, network-enabled computer devices may include an iPhone, iPod, iPad from Apple® or any other mobile device running

Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[0094] The user device 520 may include a processor 521, a memory 522, and an application 523. The processor 521 may be a processor, a microprocessor, or other processor, and the user device 520 may include one or more of these processors. The processor 521 may include processing circuitry, which may contain additional components, including additional processors, memories, error and parity/CRC checkers, data encoders, anti-collision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein.

[0095] The processor 521 may be coupled to the memory 522. The memory 522 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the user device 520 may include one or more of these memories. A read-only memory may be factory programmable as read-only or one-time programmable. One-time programmability provides the opportunity to write once then read many times. A write-once read-multiple memory may be programmed at a point in time after the memory chip has left the factory. Once the memory is programmed, it may not be rewritten, but it may be read many times. A read/write memory may be programmed and re-programmed many times after leaving the factory. It may also be read many times. The memory 522 may be configured to store one or more software applications, such as the application 523, and other data, such as user's shopping and financial account information.

[0096] The application 523 may comprise one or more software applications, such as a package delivery application and a contactless card reading application, comprising

instructions for execution on the user device 520. In some examples, the user device 520 may execute one or more applications, such as software applications, that enable, for example, network communications with one or more components of the system 500, transmit and/or receive data, and perform the functions described herein. Upon execution by the processor 521, the application 523 may provide the functions described in this specification, specifically to execute and perform the steps and functions in the process flows described below. For example, the package delivery application of the application 523 may be executed to perform retrieving information of a package delivery stored in the database 540; the contactless card reading application of the application 523 may be executed to perform communications with the contactless card 510. Such processes may be implemented in software, such as software modules, for execution by computers or other machines. The application 523 may provide GUIs through which a user may view and interact with other components and devices within the system 500. The GUIs may be formatted, for example, as web pages in HyperText Markup Language (HTML), Extensible Markup Language (XML) or in any other suitable form for presentation on a display device depending upon applications used by users to interact with the system 500.

[0097] The user device 520 may further include a display 524 and input devices 525. The display 524 may be any type of device for presenting visual information such as a computer monitor, a flat panel display, and a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays. The input devices 525 may include any device for entering information into the user device 520 that is available and supported by the user device 520, such as a touch-screen, keyboard, mouse, cursor-control device, touch-screen, microphone, digital camera, video recorder or camcorder. These devices

may be used to enter information and interact with the software and other devices described herein. For example, the input devices 525 may comprise a card reader. The card reader may be configured to read from and/or communicate with the contactless card 510. In conjunction with the application 523, the card reader may communicate with the contactless card 510 using short-range wireless communication (e.g., NFC).

[0098] The server 530 may be a network-enabled computer device. The server 530 may include a processor 531, a memory 532, and an application 533. The server 530 may further include a display 534 and input devices 535. In some examples, the server 530 is similar to the server 130 in Figure 1.

[0099] The database 540 may be one or more databases configured to store data, including without limitation, private information of users, financial accounts of users, identities of users, transactions of users, and certified and uncertified documents. In some examples, the database 540 is similar to the database 140 in Figure 1.

[0100] The delivery device 550 may be a network-enabled computer device. The delivery device 550 may include a processor 551, a memory 552, and an application 553. The delivery device 550 may further include a display 554 and input devices 555. In some example, the delivery device 550 is similar to the delivery device 120 in Figure 1.

[0101] The system 500 may include one or more networks 560. The one or more networks 560 are similar to the networks 150 in Figure 1.

[0102] In some examples, the contactless card 510 may be associated with a user and can be used by that user, for example, a customer to whom a package is delivered. The user device 520 may be associated with the user that owns the contactless card 510. The server 530 can be associated with a financial institution, such as a bank or a credit card company that offers

financial services to the user of the contactless card 510. The contactless card 510 may be issued by the financial institution. The delivery device 550 can be associated with a package delivery person and may be operated by that person, such as a delivery person of a courier.

[0103] Figure 6 illustrates a sequence diagram 600 of contactless package delivery according to an example embodiment. Figure 6 may reference the same or similar components as those illustrated in Figures 1-5, including a contactless card, a user device, a delivery device, a server, a database, and a network.

[0104] In step 610, a contactless card (e.g., the contactless card 510) transmits a cryptogram after entry of the contactless card into a communication field of a user device (e.g., the user device 520). The contactless card may be tapped by a user to the user device. The user device may be configured to have a card reader to read a cryptogram from the contactless card upon the tap. The card reader may comprise a communication interface to generate a communication field of the card reader. As used herein, a tap of the contactless card to the user device may not indicate that the contactless card is in a physical contact with the user device. A tap of the contactless card to the user device may refer to entry of the contactless card into the communication field of the card reader. The cryptogram may be stored in a memory of the contactless card. The cryptogram may be associated with a unique identifier of a user account.

[0105] In step 615, the user device may transmit the cryptogram to a server (e.g., the server 530). Upon reading the cryptogram from the contactless card, the user device transmits the cryptogram to the server via a network (e.g., the network 560). Prior to transmission, the cryptogram may be encrypted by the contactless card.

[0106] In step 620, the server validates the cryptogram, decrypts the cryptogram and extracts the unique identifier. When the server receives the cryptogram, the server may decrypt the

cryptogram after verifying the cryptogram. The server may then extract the unique identifier of the user account.

[0107] In step 625, the server may query, using the unique identifier, for an identity of the user account. In this step, the server communicates with a database (e.g., the database 540) for searching for the identity of the user account. The identity of the user account is stored on the database. The identity of the user account may comprise a name of the user who taps the contactless card. The user account may comprise one or more email addresses associated with the user, a phone number of the user, a mailing address of the user, and so forth. Once the identity of the user account matches the unique identifier of the user account, the user of the contactless card is verified.

[0108] In step 630, the server may generate a digital signature based on the identity of the user account. After obtaining and verifying the identity of the user account, the server may be configured to generate a digital signature of the identity. The digital signature may be a signature of the user name or other signatures associated with the user name.

[0109] In step 635, the server may transmit a verification notification including the identity of the user account and the digital signature to the delivery device. The verification notification may indicate that the user of the contactless card has been verified, what the identity of the user is, and the digital signature of the identity. When the delivery device receives the verification notification, the delivery device may display the verification notification on the display of the delivery device. The delivery device may be configured to sign a package receipt document using the digital signature.

[0110] Figure 7 illustrates a flow chart for a method 700 of contactless package delivery according to an example embodiment. Figure 7 may reference the same or similar components

as those illustrated in Figures 1-6, including a contactless card, a user device, a delivery device, a server, a database, and a network. The method 700 may be implemented in the system 500 and may comprise the following steps.

[0111] In step 705, a contactless card transmits a cryptogram to a server via an intermediary device. The intermediary device may comprise a user device (e.g., the user device 520). Communication between the user device and the contactless card may involve the contactless card being sufficiently close to a card reader of the user device to enable near field communication (NFC) data transfer between the user device and the contactless card.

[0112] In step 710, the server validates the cryptogram. In step 715, the server decrypts the cryptogram. In step 720, the server extracts the unique identifier from the decrypted cryptogram. In step 725, the server queries, using the unique identifier, a database (e.g., the database 540) for an identity of the user account. In step 730, the server generates a digital signature based on the identity of the user account. The steps 705-730 are similar to the steps 305-330 in Figure 3. Details of the steps 705-730 are not repeated herein.

[0113] In step 735, the server transmits a verification notification including the identity of the user account and the digital signature to the delivery device. The verification notification may indicate that the user/customer who tapped the contactless card to the user device has been verified. When receiving the verification notification, the delivery device may display the verification notification on a display of the delivery device. The delivery device may display the digital signature next to the user/customer name to whom the package is delivered. This digital signature may be considered as an authorization and verification for releasing the package to the user.

[0114] In some embodiments, one or more authentication factors may be used to verify the

identity of the user/user account in addition to the unique identifier as used in Figure 7. Figure 8 illustrates a flow chart for a method 800 of contactless package delivery according to an example embodiment. In the method 800, one or more authentication factors may be used to verify the identity of the user/user account. Figure 8 may reference the same or similar components as those illustrated in Figures 1-7, including a contactless card, a user device, a delivery device, a server, a database, and a network. The method 800 may be implemented in the system 500 and may comprise the following steps.

[0115] The method 800 may include: a contactless card transmits a cryptogram to a server via an intermediate device (the user device 520; step 805); the server validates the cryptogram (step 810); the server decrypts the cryptogram (step 815); the server extracts the unique identifier (step 820); the server queries, using the unique identifier, a database for an identity of the user account (step 825); the server receives from the database, one or more authentication factors to verify the identity of the user account (step 830); the server generates a digital signature based on the identity of the user account (step 835); and the server transmits a verification notification including the identity of the user account and the digital signature (step 840). The steps 805-825 and 835-840 are similar to the corresponding steps 705-725 and 730-735, details of which are not repeated herein.

[0116] In step 830, the one or more authentication factors may be provided by the user device 520 and/or the delivery device 550. For example, the user device 520 may transmit to the server a geo-signature of the user device 520; and the delivery device 550 may transmit to the server a geo-signature of the delivery device 550. The server may compare the geo-signature of the user device with the geo-signature of the delivery device, and generate the digital signature based on the comparison.

[0117] The one or more authentication factors may also comprise at least one selected from the group of a password, a personal identification (PIN), and a biometric feature. The server may verify the identity of the user account based on the one or more authentication factors.

[0118] In some embodiments, the delivery device 550 may transmit a card tapping notification through the server to the user device 520. For example, when a package delivery person is approaching or at a package pickup location (e.g., the user's home address/the package delivery address), the delivery person may operate the delivery device to transmit a card tapping notification to the user device. When receiving the card tapping notification, the user may tap the contactless card to the user device. . Figure 9 describes a method 900 of contactless package delivery based on a card tapping notification according to an example embodiment. Figure 9 may reference the same or similar components as those illustrated in Figures 1-8, including a user device, a server, a database, and a delivery device.

[0119] In step 905, the server may receive a card tapping notification. The card tapping notification may be initiated by the delivery device and transmitted to the server. Upon receiving the card tapping notification, the server may forward/transmit the card tapping notification to the user device and prompt to read the contactless card. The user of the user device may then tap the contactless card to the user device in accordance with the card tapping notification.

[0120] In step 910, the server may read the contactless card based on the card tapping notification. For example, after the contactless card being tapped to the user device, the user device may receive a cryptogram from the contactless card and then transmit the cryptogram to the server.

[0121] In step 915, the server may receive a tapping-completed notification from the user

device. After the contactless card being tapped, the user device may generate a card tapping-completed notification that is then transmitted to the server. The server may transmit the card tapping-completed notification to the delivery device, such that the delivery person is informed that the contactless card has been tapped to the user device.

[0122] In step 920, the server may generate the digital signature of the identity of the user account using the tapping-completed notification. For example, the cryptogram may be verified by the server and the identity of the user account may be retrieved by the server, as described above. The server may further verify the identity of the user account/user based on the card tapping-completed notification, and then generate the digital signature of the identity of the user.

[0123] In some embodiments, the delivery device 550 may transmit a universal resource locator (URL) link for card tapping through the server to the user device 520. For example, when a package delivery person is approaching or at a package pickup location (e.g., the user's home address/the package delivery address), the delivery person may operate the delivery device to transmit a URL link for card tapping to the user device. When receiving the URL link for card tapping, the user may tap the contactless card to the user device. . Figure 10 describes a method 1000 of contactless package delivery based on a URL link for card tapping according to an example embodiment. Figure 10 may reference the same or similar components as those illustrated in Figures 1-9, including a user device, a server, a database, and a delivery device.

[0124] In step 1005, the server may receive a URL link for card tapping. The URL link for card tapping may be initiated and transmitted by the delivery device to the server. Upon receiving the URL link, the server may forward/transmit the URL link to the user device.

[0125] In step 1010, the user of the user device may open the URL link to display a web page, and then tap the contactless card to the user device via the web page.

[0126] In step 1015, the server may read the contactless card. For example, after the contactless card being tapped to the user device via the web page, the user device may receive a cryptogram from the contactless card and then transmit the cryptogram to the server. For example, the web page may comprise java script, and the java script interacts with the underlying native platform of the web browser to trigger the NFC read. The web page would then take the contents of that NFC read and deliver it to the server.

[0127] In step 1020, the server may receive a tapping-completed notification from the user device. After the contactless card being tapped, the user device may generate a card tapping-completed notification via the web page that is then transmitted to the server. The server may transmit the card tapping-completed notification to the delivery device, such that the delivery person is informed that the contactless card has been tapped to the user device.

[0128] In step 1025, the server may generate the digital signature of the identity of the user account using the tapping-completed notification. For example, the cryptogram may be verified by the server and the identity of the user account may be retrieved by the server, as described above. The server may further verify the identity of the user account/user based on the card tapping-completed notification, and then generate the digital signature of the identity of the user.

[0129] In some embodiments, the contactless card may embody host card emulation. For example, the user device 520 in Figure 5 may emulate the contactless card, as opposed to functioning as a reader for the contactless card. In this example, the user device 520 may function as the contactless card and can be tapped to other devices (e.g., the delivery device

120 or the delivery device 550). Accordingly, instead of authenticating the user through one or more second factors, the delivery device can communicate with the server to determine the identity of the user and verify against an expected delivery.

[0130] In some examples, the user device emulating the contactless card can also operate anonymously or in an identified manner, but in either case can limit personal information exposure. The delivery device may access the server using a request service for verifying the user. The server may reply with a determination indicating whether the user is verified. The delivery device may also submit the delivery address for the package to the server that can be used to match on the database the identity with the contactless card identifier.

[0131] In some embodiments, a profile picture of the user may be transmitted after tapping a contactless card. For example, when the user enters or drives towards a store, the user could tap his/her contactless card on a card reader and the contactless card may send the profile picture of the user to a store employee. The store employee may send the user a picture of himself or herself based on information that is stored with the user's profile. In this way, the user is able to recognize the store employee from across the store without a physical contact with the person. If some close interaction is required, the user and the store employee will have been informed of each other and expeditiously proceed with the interaction without passing by or encountering other people.

[0132] In some embodiments, the digital signature can be a direct or indirect signature. For example, the direct signature refers to a signature of the known recipient of the delivery package (or someone associated with the known recipient's account), and the indirect signature refers to a signature of a person other than the known recipient of the delivery package. For example, if a person who is not on the delivery package can tap his or her contactless card, his

or her name can be applied as an indirect signature. If this indirect signature can satisfy the delivery condition, a notification may be sent to the known recipient of the delivery package indicating the package has been signed by that person. But if the delivery requires a direct signature, the system can require the known recipient to sign, and the known recipient who is on the delivery package can then tap his/her contactless card.

[0133] In some embodiments, multiple tapping of a contactless card may be desired to prevent a replay attack. As used herein, the replay attack may refer to the unauthorized interception of a cryptogram message and cloning of this message for use in signing for packages. For example, the cryptogram message can be read and then statically programmed into a writable NFC tag, which can provide the same cryptogram when read repeatedly (without generating a new counter).

[0134] By tapping the contactless card multiple times (e.g., twice by the user), the cryptogram messages can be verified to be genuinely generated by the contactless card even if no a second authentication factor is entered, because if the contactless card is tapped multiple times, then the server has multiple successive cryptogram messages to compare. In this way, the multiple successive cryptogram messages can be validated that they were actually generated by the card and not a static replay of a single cryptogram message.

[0135] This can enhance security when second authentication factors are not available. For example, when a user taps his or her random card to some random person's device, a second authentication factor is not available. In such scenarios, by tapping a card multiple times, the card can be validated to be a card that is being used to generate the cryptograms.

[0136] In some embodiments, after recording the digital signature that this has happened, the actual cryptogram message that was used to generate that signature may be stored, for example,

on the database. The stored cryptogram message can serve as an audit mechanism because the stored cryptogram message can be revalidated. With the authentication mechanism of the contactless card, the current cryptogram message being authenticated is in the right counter range. Accordingly, the validation is able to establish that that message was once created by the contactless card.

[0137] In some embodiments, the recording of the cryptogram messages may act as a ledger of confirmation that the package was delivered if, for example, there is a dispute over whether or when a package has been delivered and who signed for it. For example, a customer may claim he or she received the package on a particular day within the time window specified by a return policy. However, referencing the stored cryptogram message, the merchant that shipped the package may establish that the customer in fact received the package on a prior day and therefore the return policy does not apply.

[0138] In some embodiments, a delivery address may be certified to act as a delivery requirement. For example, a package may be required to deliver to the certified address (e.g., a digitally signed address).

[0139] In some embodiments, certain conditions may need to be met for the digital signature to be applicable. For example, a product may have an expiration date, a guaranteed delivery date, and/or restrictions about how long it can be in transportation. For example, if a product subject to such restrictions (e.g., medicine, test samples, or perishable items) is not delivered within a certain time then, the conditions will not allow a consumer to sign for that product.

[0140] In some embodiments, the signed certificates can be scoped to a particular delivery transaction and enforce conditions and requirements of the delivery transaction. For example, a merchant can apply requirements that a package be delivered to a certain address or that the

package delivery has these particular restrictions, the identity of that person signing for the package can be validated against those requirements. For example, a customer expecting a time-sensitive package may contract with a delivery company for a particular delivery date and time and the customer may not wish to take delivery of a package after the specified time. In such an example, the customer can prove at the time of delivery that the contract has been violated.

[0141] Throughout the disclosure, the term merchant is used, and it is understood that the present disclosure is not limited to a particular merchant or type of merchant. Rather, the present disclosure includes any type of merchant, vendor, or other entity involving in activities where products or services are sold or otherwise provided.

[0142] In some examples, exemplary procedures in accordance with the present disclosure described herein can be performed by a processing arrangement and/or a computing arrangement (e.g., computer hardware arrangement). Such processing/computing arrangement can be, for example entirely or a part of, or include, but not limited to, a computer/processor that can include, for example one or more microprocessors, and use instructions stored on a computer-accessible medium (e.g., RAM, ROM, hard drive, or other storage device). For example, a computer-accessible medium can be part of the memory of the delivery device 120 or 550, the user device 520, the server 130 or 530, and/or the contactless card 110 or 510 or other computer hardware arrangement.

[0143] In some examples, a computer-accessible medium (e.g., as described herein above, a storage device such as a hard disk, floppy disk, memory stick, CD-ROM, RAM, ROM, etc., or a collection thereof) can be provided (e.g., in communication with the processing arrangement). The computer-accessible medium can contain executable instructions thereon.

In addition or alternatively, a storage arrangement can be provided separately from the computer-accessible medium, which can provide the instructions to the processing arrangement so as to configure the processing arrangement to execute certain exemplary procedures, processes, and methods, as described herein above, for example.

[0144] Throughout the disclosure, the following terms take at least the meanings explicitly associated herein, unless the context clearly dictates otherwise. The term “or” is intended to mean an inclusive “or.” Further, the terms “a,” “an,” and “the” are intended to mean one or more unless specified otherwise or clear from the context to be directed to a singular form.

[0145] In this description, numerous specific details have been set forth. It is to be understood, however, that implementations of the disclosed technology may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description. References to “some examples,” “other examples,” “one example,” “an example,” “various examples,” “one embodiment,” “an embodiment,” “some embodiments,” “example embodiment,” “various embodiments,” “one implementation,” “an implementation,” “example implementation,” “various implementations,” “some implementations,” etc., indicate that the implementation(s) of the disclosed technology so described may include a particular feature, structure, or characteristic, but not every implementation necessarily includes the particular feature, structure, or characteristic. Further, repeated use of the phrases “in one example,” “in one embodiment,” or “in one implementation” does not necessarily refer to the same example, embodiment, or implementation, although it may.

[0146] As used herein, unless otherwise specified the use of the ordinal adjectives “first,” “second,” “third,” etc., to describe a common object, merely indicate that different instances

of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

[0147] While certain implementations of the disclosed technology have been described in connection with what is presently considered to be the most practical and various implementations, it is to be understood that the disclosed technology is not to be limited to the disclosed implementations, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

[0148] This written description uses examples to disclose certain implementations of the disclosed technology, including the best mode, and also to enable any person skilled in the art to practice certain implementations of the disclosed technology, including making and using any devices or systems and performing any incorporated methods. The patentable scope of certain implementations of the disclosed technology is defined in the claims, and may include other examples that occur to those skilled in the art. Such other examples are intended to be within the scope of the claims if they have structural elements that do not differ from the literal language of the claims, or if they include equivalent structural elements with insubstantial differences from the literal language of the claims.

CLAIMS

What is claimed is:

1. A contactless delivery system, comprising:
 - a contactless card comprising a processor and a memory, the memory storing a cryptogram that contains an unique identifier associated with a user account,
 - wherein, after entry into a communication field, the contactless card is configured to transmit the cryptogram to a server via one or more intermediary devices, and
 - wherein, upon receipt of the cryptogram, the server is configured to:
 - validate the cryptogram,
 - decrypt the cryptogram and extract the unique identifier,
 - query, using the unique identifier, a database for an identity of the user account,
 - generate a digital signature based on the identity of the user account, and
 - transmit a verification notification including the identity of the user account and the digital signature.
2. The contactless delivery system of claim 1, wherein the one or more intermediary devices comprise a communication interface configured to generate the communication field.
3. The contactless delivery system of claim 1, wherein:
 - the memory further contains a counter value and a plurality of keys, and
 - the processor of the contactless card is configured to generate the cryptogram using the counter value, the plurality of keys, and the unique identifier.

4. The contactless delivery system of claim 3, wherein
the processor of the contactless card is configured to update the counter value.
5. The contactless delivery system of claim 1, wherein:
the verification notification is transmitted to a user device storing information on a delivery package, and
the server is further configured to receive the information on the delivery package as an authentication factor to verify the identity of the user account.
6. The contactless delivery system of claim 1, wherein the database contains one or more documents associated with the user account, the one or more documents comprising a copy of a driver license.
7. The contactless delivery system of claim 6, wherein the server is configured to receive, from the database, the one or more documents to verify the identity of the user account.
8. The contactless delivery system of claim 1, wherein:
the server is configured to transmit the verification notification to a user device, and
the digital signature is displayed on a display of the user device, the digital signature being used to sign a package receipt document displayed on the display of the user device.

9. The contactless delivery system of claim 1, wherein the contactless card includes a host card emulation device emulating the contactless card.

10. The contactless delivery system of claim 1, wherein the server is configured to:

retrieve a profile picture of the user account from the database, and
transmit the profile picture to verify the identity of the user account.

11. The contactless delivery system of claim 1, wherein the server is further configured to:

retrieve a document of the user account from the database, and
transmit the document to verify the identity of the user account.

12. A contactless delivery system, comprising:

a server comprising a processor and a memory, wherein the server is configured to:
receive a cryptogram containing an unique identifier associated with a user
account,

validate the cryptogram,

decrypt the cryptogram and extract the unique identifier,

query, using the unique identifier, a database for an identity of the user
account,

generate a digital signature based on the identity of the user account, and

transmit a verification notification including the identity of the user account
and the digital signature.

13. The contactless delivery system of claim 12, wherein:
- the cryptogram is stored on a contactless card; and
 - the server is configured to receive the cryptogram via an intermediary device configured to generate a communication field for data communication with the contactless card.
14. The contactless delivery system of claim 13, wherein the server is configured to receive a geo-signature of the intermediary device.
15. The contactless delivery system of claim 14, wherein the server is further configured to:
- receive a geo-signature of a user device,
 - compare the geo-signature of the intermediary device with the geo-signature of the user device, and
 - generate the digital signature based on the comparison.
16. The contactless delivery system of claim 12, wherein the server is configured to:
- receive one or more authentication factors, the one or more authentication factors comprising at least one selected from a group of a password, a personal identification (PIN), and a biometric feature, and
 - verify the identity of the user account based on the one or more authentication factors.
17. The contactless delivery system of claim 12, wherein the server is configured to:
- receive a card tap notification;

prompt to read a contactless card based on the card tap notification;
receive a tap-completed notification; and
generate the digital signature of the identity of the user account using the tap-completed notification.

18. The contactless delivery system of claim 12, wherein the server is configured to:

receive a universal resource locator (URL) link,
open the URL link to display a web page,
read a contactless card through the web page, and
generate the digital signature of the identity of the user account using the web page.

19. A contactless delivery method, comprising:

receiving a cryptogram, the cryptogram containing an unique identifier associated with a user account;
validating the cryptogram;
decrypting the cryptogram and extracting the unique identifier;
querying, using the unique identifier, a database for an identity of the user account,
generating a digital signature based on the identity of the user account; and
transmitting a verification notification including the identity of the user account and the digital signature.

20. The contactless delivery method of claim 19, comprising receiving an additional cryptogram.