(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 August 2022 (04.08.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/164951 A1

(51) International Patent Classification:
H04L 9/40 (2022.01) *H04W 12/06* (2021.01)
H04L 67/02 (2022.01) *G06F 21/35* (2013.01)
H04W 4/80 (2018.01) *G06Q 20/34* (2012.01)

(21) International Application Number:
PCT/US2022/013978

(22) International Filing Date:
27 January 2022 (27.01.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17/162,783 29 January 2021 (29.01.2021) US

(71) Applicant: **CAPITAL ONE SERVICES, LLC** [US/US]; 1680 Capital One Dr., McLean, Virginia 22102 (US).

(72) Inventors: **HART, Colin**; 1680 Capital One Dr., McLean, Virginia 22102 (US). **BERGERON, George**; 1680 Capital One Drive, McLean, Virginia 22102 (US). **NEWMAN, Kaitlin**; 1680 Capital One Drive, McLean, Virginia 22102 (US). **RULE, Jeffrey**; 1680 Capital One Drive, McLean, Virginia 22102 (US).

(74) Agent: **KASNEVICH, Andrew D.** et al.; Hunton Andrews Kurth LLP, Intellectual Property Department, 2200 Pennsylvania Ave., NW, Washington, District of Columbia 20037 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,

(54) Title: SYSTEMS AND METHODS FOR AUTHENTICATED PEER-TO-PEER DATA TRANSFER USING RESOURCE LOCATORS

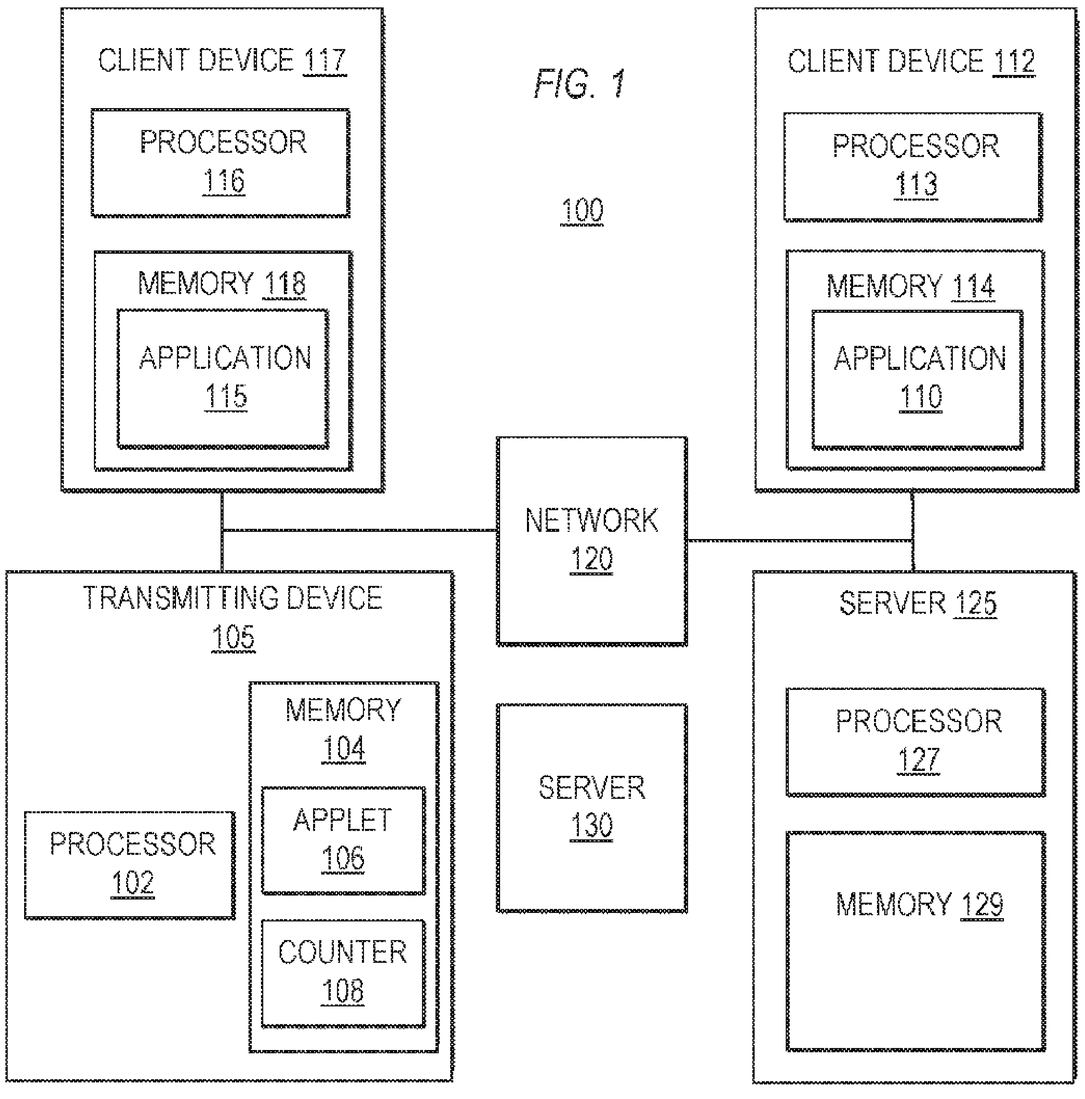


FIG. 1

100

(57) Abstract: An authenticated data transfer system may include generating, after entry of one or more processors of a transmitting device into a communication field, a link, the link comprising a near field communication data exchange format uniform resource locator including identifier data and user data; transmitting, to a first application comprising instructions for execution on a first device, the link to initiate data transfer; authenticating a user associated with the first device by activating one or more actions based on the link; transmitting one or more requests for confirmation of quantity and recipient data associated with the data transfer; receiving one or more notifications that are based on the one or more requests for confirmation of quantity and recipient data associated with the data transfer; and performing one or more login credentials that are responsive to the one or more notifications so as to complete the data transfer.

[Continued on next page]

WO 2022/164951 A1

ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

SYSTEMS AND METHODS FOR AUTHENTICATED PEER-TO-PEER DATA TRANSFER USING RESOURCE LOCATORS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Patent Application No. 17/162,783 filed January 29, 2021, the disclosure of which is incorporated herein by reference in its entirety.

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates to systems and methods for peer-to-peer data transfers, and in particular, authenticated peer-to-peer data transfer using resource locators.

BACKGROUND

[0003] When two peer devices are not already connected through an existing network, peer-to-peer data transfers may be cumbersome. This is because both peer devices must be registered with and configured for communication on the same network in order to accomplish the transfer. In addition, configuring and scheduling the transfer of data may be detrimental to the user experience. Security risks are also present, and may include risks associated with data integrity and vulnerability when crossing between platforms, and the misidentification of an account by the use of an email address or other account identifier. These risks and shortcomings may reduce user demand for cross-application communication and inhibit the functionality and efficiency of cross-application communications.

[0004] These and other deficiencies exist. Accordingly, there is a need for systems and methods for peer-to-peer data transfer that provide enhanced security and an improved user experience.

SUMMARY OF THE DISCLOSURE

[0005] Embodiments of the present disclosure provide an authenticated data transfer system, including a contactless card comprising a processor and a memory. After entering a

communication field, the processor may be configured to dynamically generate a uniform resource locator (URL). The URL may include a first set of information including abstracted identifier information. The URL may include a second set of information including user information. The processor may be configured to transmit the URL to initiate data transfer. The data transfer may be completed upon verification of a received response and confirmation of a third set of information associated with the data transfer.

[0006] Embodiments of the present disclosure provide a method of authenticating data transfer. The method may include dynamically generating, after entry of one or more processors of a transmitting device into a communication field, the link comprising a near field communication data exchange format uniform resource locator including identifier data and user data. The method may include transmitting, to a first application comprising instructions for execution on a first device, the link to initiate data transfer. The method may include authenticating a user associated with the first device by activating one or more actions based on the link. The method may include transmitting one or more requests for confirmation of quantity and recipient data associated with the data transfer. The method may include receiving one or more notifications that are based on the one or more requests for confirmation of quantity and recipient data associated with the data transfer. The method may include performing one or more login credentials that are responsive to the one or more notifications so as to complete the data transfer.

[0007] Embodiments of the present disclosure provide a computer readable non-transitory medium comprising computer-executable instructions that, when executed by a processor, perform procedures comprising the steps of: dynamically generating, after entry of a contactless card into a communication field, a link, the link comprising a first set of information and a second set of information, the first set of information including identifier information, the second set of

information including user information; transmitting, to a first application comprising instructions for execution on a first device, the link to initiate data transfer; identifying a user associated with the first device by activating one or more actions based on the link, the one or more actions configured to request confirmation of a third set of information associated with the data transfer; and transmitting one or more responses based on authentication of the third set of information so as to complete the data transfer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Various embodiments of the present disclosure, together with further objects and advantages, may best be understood by reference to the following description taken in conjunction with the accompanying drawings.

[0009] Figure 1 depicts an authenticated data transfer system according to an exemplary embodiment.

[00010] Figure 2A is an illustration of a contactless card according to an exemplary embodiment.

[00011] Figure 2B is an illustration of a contact pad of the contactless card according to an exemplary embodiment.

[00012] Figure 3 depicts a method of authenticating data transfer according to an exemplary embodiment.

[00013] Figure 4 depicts a method of initiating and authenticating data transfer according to an exemplary embodiment.

[00014] Figure 5 depicts another method of initiating and authenticating data transfer according to an exemplary embodiment.

DETAILED DESCRIPTION

[00015] 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.

[00016] As disclosed herein, a user may use their card to for seamless identification and to also initiate a data transfer. A resource locator, such as a uniform resource locator (URL), internet resource locator (IRL), uniform resource identifier (URI), uniform resource name (URN), or other resource locator, may include abstracted identification information, including but not limited to an account or user identifier for a cardholder, which is loaded onto the chip at the time of personalization of the card. The abstracted identification information may be generated for each transaction, such as the dynamically generated URL.

[00017] Without limitation, the identification information may be generated on the card by combining a unique identifier with one or more variables, such as a counter, one or more cryptographic algorithms, and/or any combination thereof. For example, the one or more cryptographic algorithms may include an encryption technique, such as public or private key encryption, that would also be known by a server for authentication. Without limitation, exemplary symmetric key algorithms may include symmetric key encryption such as DES (Data Encryption

Standard), Triple DES, or AES (Advanced Encryption Standard). Without limitation, exemplary asymmetric key algorithms may include asymmetric public key encryption, digital signature algorithm, or RSA (Rivest–Shamir–Adleman).

[00018] In some examples, the peer-to-peer data transfer may be initiated and authenticated through a website. In other examples, the peer-to-peer data transfer may be initiated and authenticated through an application. The systems and methods disclosed herein minimize the exposure of identification information or other personal information and provide greater security.

[00019] Example embodiments of the present disclosure provide improvements to the limitations in the user experience to set up and coordinate different types of data transfer, and mitigate or eliminate security risks, such as those associated with crossing between platforms, misidentification of an account by email address, authentication of the requested transfer of data, and validity of device recognition. Accordingly, the systems and methods disclosed herein improve upon existing implementations by coordinating customized peer-to-peer data transfer that addresses these limitations and provides enhanced security benefits and an improved user experience.

[00020] Figure 1 illustrates an authenticated data transfer system 100. The authenticated data transfer system 100 may comprise a transmitting device 105, a first application 110, a second application 115, a network 120, a server 125, and a database 130. Although Figure 1 illustrates single instances of components of system 100, system 100 may include any number of components.

[00021] System 100 may include a transmitting device 105. The transmitting device 105 may comprise a contactless card, a contact-based card, a network-enabled computer, or other device described herein. As further explained below in FIGs. 2A-2B, transmitting device 105 may include

one or more processors 102, and memory 104. Memory 104 may include one or more applets 106 and one or more counters 108. Transmitting device 105 may be in data communication with one or more devices 112, 117. For example, transmitting device may transmit data via network 120 to client devices 112, 117. In some examples, transmitting device 105 may be configured to transmit data via network 120 to client device 117 after entry into one or more communication fields of client devices 112, 117. Without limitation, transmitting device 105 may be configured to transmit data to client devices 112, 117 after one or more entries into the one or more communication fields of client devices 112, 117, the one or more entries associated with a tap, a swipe, a wave, and/or any combination thereof.

[00022] System 100 may include a first application 110. For example, first application 110 may comprise instructions for execution on a first device 112. First application 110 may be in communication with any components of system 100. For example, first device 112 may execute one or more applications, such as first application 110, that enable, for example, network and/or data communications with one or more components of system 100 and transmit and/or receive data. The first device 112 may include one or more processors 113 coupled to memory 114. For example, first device 112 may be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a handheld PC, a personal digital assistant, a contactless card, a thin client, a fat client, an Internet browser, or other device. First device 112 also may be a mobile device; for example, a mobile device 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.

[00023] The first device 112 may include processing circuitry and 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. The first device 112 may further include a display and input devices. The display 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 may include any device for entering information into the user's device that is available and supported by the user's device, 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. In some examples, the first device 112 may include at least one selected from the group of a mobile device, a wearable device, and a kiosk.

[00024] System 100 may include a second application 115. Second application 115 may comprise instructions for execution on a second device 117. Second application 115 may be in communication with any components of system 100. For example, second device 117 may execute one or more applications, such as second application 115, that enable, for example, network and/or data communications with one or more components of system 100 and transmit and/or receive data. The second device 117 may include one or more processors 116 coupled to memory 118. For example, second device 117 may be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device

including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a handheld PC, a personal digital assistant, a contactless card, a thin client, a fat client, an Internet browser, or other device. Second device 117 also may be a mobile device; for example, a mobile device 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.

[00025] The second device 117 may include processing circuitry and 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. The second device 117 may further include a display and input devices. The display 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 may include any device for entering information into the user's device that is available and supported by the user's device, 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. In some examples, the second device 117 may include at least one selected from the group of a mobile device, a wearable device, and a kiosk.

[00026] System 100 may include a network 120. In some examples, network 120 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 to any one of components of system 100. For example,

client devices 112, 117 may be configured to connect to server 125 via network 120. In some examples, network 120 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.

[00027] In addition, network 120 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, network 120 may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. Network 120 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. Network 120 may utilize one or more protocols of one or more network elements to which they are communicatively coupled. Network 120 may translate to or from other protocols to one or more protocols of network devices. Although network 120 is depicted as a single network, it should be appreciated that according to one or more examples, network 120 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.

[00028] Client devices 112, 117 may be in communication with one or more servers 125 via one or more networks 120, and may operate as a respective front-end to back-end pair with server 125.

Client devices 112, 117 may transmit, for example from a mobile device application 110, 115 executing thereon, one or more requests to server 125. The one or more requests may be associated with retrieving data from server 125. Server 125 may receive the one or more requests from client devices 112, 117. Based on the one or more requests from client applications 110, 115, server 125 may be configured to retrieve the requested data. Server 125 may be configured to transmit the received data to client applications 110, 115, the received data being responsive to one or more requests.

[00029] System 100 may include one or more servers 125. In some examples, server 125 may include one or more processors 127 coupled to memory 129. Server 125 may be configured as a central system, server or platform to control and call various data at different times to execute a plurality of workflow actions. Server 125 may be configured to connect to one or client devices 112, 117. Server 125 may be in data communication with the client applications 110, 115. For example, a server 125 may be in data communication with the client applications 110, 115 via one or more networks 120.

[00030] System 100 may include one or more databases 130. The database 130 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 130 may comprise a desktop database, a mobile database, or an in-memory database. Further, the database 130 may be hosted internally by the devices 112, 117 or the database 130 may be hosted externally to the devices 112, 117, such as by a server 125, by a cloud-based platform, or in any storage device that is in data communication with the devices 112, 117. In some examples, database 130 may be in data communication with any number of components of system 100. For example, server 125 may be configured to retrieve the requested

data from the database 130 that is transmitted by applications 110, 115. Server 125 may be configured to transmit the received data from database 130 to client applications 110, 115 via network 120, the received data being responsive to the transmitted one or more requests. In other examples, client applications 110, 115 may be configured to transmit one or more requests for the requested data from database 130 via network 120.

[00031] 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 client devices 112, 117 and/or server 125 or other computer hardware arrangement.

[00032] 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.

[00033] In some examples, the transmitting device 105 may comprise a contact-based card. For example, the contact-based card may be configured to transmit, after establishing a connection

with a device, a link to initiate data transfer. The link may comprise, for example, a URL, IRL, URI, or URN. Without limitation, the contact-based card may be configured to establish physical contact with a card reader of client device 112 (e.g., a chip reader or a magnetic stripe reader). The card reader may be integral, within, or external to the client device 112.

[00034] In other examples, the transmitting device 105 may comprise a contactless card. For example, the contactless card may be configured to, after entering a communication field, transmit to the first application 110, a link to initiate data transfer. The link may comprise, for example, a URL, IRL, URI, or URN. In some examples, the contactless card may enter the communication field of client device 112 via one or more gestures selected from the group of a tap, swipe, wave, or any combination thereof.

[00035] In some examples, the user may be identified based on a mobile network operator (MNO) lookup. In other examples, the user may be identified based on one or more cookies associated with prior account logins, e.g., logins to an account associated with the transmitting device, a separate account associated with the user, and/or other accounts. The link may comprise a near field communication data exchange format uniform resource locator (NDEF URL) and can be configured to invoke one or more actions or applications. In one example, the link may be configured to invoke a website, which can include causing a browser or other viewing application executing on client device 112 or another device to access and display a website and/or to cause the website to perform one or more actions (e.g., to display or submit information). In another example, the link may be configured to invoke an application executing on client device 112 or a separate device.

[00036] The link may comprise a first set of information and a second set of information. For example, the first set of information may include identifier information. The first set of information

may comprise an abstracted user name generated by the processor after entry of the transmitting device 105 into the communication field. For example, the abstracted identification information may be generated for each transaction, in the form of, e.g., the dynamically generated URL. Without limitation, the identification information may be generated on the card by combining a unique identifier with one or more variables, such as a counter, one or more cryptographic algorithms, and/or any combination thereof. For example, the one or more cryptographic algorithms may include an encryption technique, such as public or private key encryption, that would also be known by a server, such as server 125, for authentication. Without limitation, exemplary symmetric key algorithms may include symmetric key encryption such as DES, Triple DES, or AES. Without limitation, exemplary asymmetric key algorithms may include asymmetric public key encryption, digital signature algorithm, or RSA. For example, the second set of information may include user information, such as cardholder information (e.g., account owner name, account number, expiration date, card verification value). The first application 110 may be configured to identify a user associated with the first device 112 by activating one or more actions based on the link. The one or more actions may be configured to request confirmation of a third set of information associated with the data transfer. The third set of information may include at least one selected from the group of a quantity, digital asset, and recipient information.

[00037] In some examples, at least one action may comprise launching a website configured to identify the user associated with the first device 112. Server 125 may be configured to identify the user associated with the first device 112 by at least one selected from the group of device fingerprinting of the first device 112 and a cookie stored on the first device 112. Without limitation, device fingerprinting may be based on at least one selected from the group of device configuration, device memory, device screen size, device operating system version, applications installed, phone

carrier provider, third party cookies for websites, phone number tracking through mobile network operator (MNO) lookup, browser type, browser language, IP address, and/or any combination thereof of the first device 112. The website may be configured to display the second set of information and the third set of information on first device 112. After a successful identification of the user or owner of the first device 112, the website may be configured to load predetermined information including the second set of information. In some examples, the predetermined information may comprise user information, such as cardholder information. In some examples, this information may be embedded in and passed via the NDEF URL when the transmitting device 105 enters the communication field. The website may be further configured to allow a quantity to be specified, including but not limited to an amount. The website may be further configured to submit the transfer by selection of a button. Moreover, the website may be further configured to adjust recipient and/or transferor of the data transfer. For example, the directionality of the data transfer may be reversed. In some examples, by adjusting the directionality of the transfer, such as from transferor to recipient or from recipient to transferor, a corresponding message such as a push notification or email may be generated so as to indicate confirmation of the desired reversed directionality of the transfer. In some examples, the corresponding message may be displayed by the first application 110 and/or second application 115.

[00038] The second application 115 may be configured to transmit one or more responses associated with authentication and confirmation of the third set of information so as to complete the data transfer. In some examples, the second application 115 may be configured to receive a notification from first application 110, the notification requiring the one or more responses associated with confirmation of the third set of information. The second application 115 may be configured to perform one or more authentication communications associated with confirmation

of the third set of information. For example, the data transfer may be completed upon verification of a received response and confirmation of the third set of information associated with the data transfer. In some examples, the one or more authentication communications may include at least one selected from the group of biometric communication and login communication.

[00039] In other examples, at least one action may comprise requesting, by the first application 110, one or more login credentials. The first application 110 may be configured to, upon submission of the requested one or more login credentials and upon authentication of the one or more login credentials, deep link to a screen with the second set of information and the third set of information. By way of example, deep linking described herein may refer to the NDEF URL being configured to link to a specific, generally searchable or indexed, portion of web content on a website, rather than a website's home page. The third set of information may include at least one selected from the group of a quantity, digital asset, and recipient information. In some examples, the second application 115 may be configured to receive a notification, the notification requiring the one or more responses associated with confirmation of the third set of information. The second application 115 may be configured to perform one or more authentication communications associated with confirmation of the third set of information. In some examples, the one or more authentication communications may include an authentication input. Exemplary authentication inputs can include, without limitation, entry of login credentials, account information, security information, biometric information and a combination thereof (e.g., entry of a user name, a password, an account number, a security code, a one-time passcode, an answer to a security question, a fingerprint, a facial scan, a retinal scan, a voice recognition, and logging into an application or website associated with an account or card-issuing institution).

[00040] The device associated with the transmitting device 105 user, such as the second

application 115 of the second device 117 associated with a cardholder, may be configured to receive a notification, including but not limited to a push notification or email, that acts as a second confirmation of the amount, digital asset, and transfer recipient. To confirm the data transfer, the cardholder may select a button to take an action that is responsive to the requested authentication communication, such as providing an authentication input. Upon authentication of the login via the received authentication input, the transfer may be confirmed. In this manner, the peer-to-peer transfer would be for an authenticated user, after the confirmation, since the transfer is to a known recipient.

[00041] In some examples, the peer-to-peer transfer may comprise issuance of credit. The credit may be in accord with one or more spending restrictions. For example, the one or more spending restrictions may include a time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof. In some examples, the issuance of credit may be associated with one or more rewards and/or points. For example, the rewards and/or points may be issued and thereby added to a user reward or loyalty point program if the credit is used at a particular merchant, such as a restaurant, at a particular time, such as on the weekends. For example, the rewards and/or points may be adjusted for each of the transferor and the transferee, and may be adjusted based on redemption of the credit. For example, the rewards and/or points may be issued and thereby added to a user reward or loyalty point program if the credit is used at a particular merchant, such as a restaurant, and/or at a particular time, such as on the weekends. When the recipient or transferee uses the credit, the transferor may still accrue the rewards and/or points.

[00042] In other examples, the peer-to-peer transfer may comprise transfer of one or more digital assets. Without limitation, the digital asset may comprise an image or a document. Without limitation, the format type of the digital asset may include at least one selected from the group of

a static image file (such as JPEG, PNG, SVG), a static document file (such as PDF, PSD), an animated file (such as GIF, SWF), and web code (such as HTML, CSS, JavaScript). The one or more digital assets may be identified for transfer. For example, the digital asset may be securely transmitted by launching a website and uploading the identified digital asset for transfer. In another example, the digital asset may be securely transmitted by opening an application or launching an email client in which the identified digital asset may be included as an attachment. In another example, digital asset may be identified as part of a uniform resource locator (URL) that is transmitted for retrieving the identified digital asset.

[00043] In other examples, the peer-to-peer transfer may comprise a funds transfer, such as a cash transfer. As with the issuance of credit, the funds transfer may be subject to one or more spending restrictions and/or one or more merchants. For example, the funds transfer may be subject to a restriction based on time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof. In some examples, the funds transfer may include a plurality of portions. For example, a first portion of the funds transfer may be transmitted prior to a second portion of the funds transfer. Any portion of the funds transfer may be transmitted at a predetermined time, including but not limited to a day, time, week, month, and/or any combination thereof. In this manner, the funds transfer may be transmitted in aggregate until satisfaction of the entire funds transfer.

[00044] In other examples, the peer-to-peer transfer may comprise issuance of a virtual gift card. As with the issuance of credit, the virtual gift card may be subject to one or more spending restrictions and/or one or more merchants. For example, the virtual gift card may be subject to time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof. In some examples, the peer-to-peer transfer may include a plurality of portions associated

with various amounts of the virtual gift card. For example, a first portion of the peer-to-peer transfer may be transmitted prior to a second portion of the peer-to-peer transfer. Any portion of the transfer may be transmitted at a predetermined time, including but not limited to a day, time, week, month, and/or any combination thereof.

[00045] FIG. 2A illustrates one or more transmitting devices 200. Transmitting device 200 may reference the same or similar components of transmitting device or contactless card 105, as explained above with respect to FIG. 1. Although Figure 2A and 2B illustrate single instances of components of transmitting device 200, any number of components may be utilized.

[00046] Transmitting device 200 may be configured to communicate with one or more components of system 100. Transmitting device 200 may comprise a contact-based card or contactless card, which may comprise a payment card, such as a credit card, debit card, or gift card, issued by a service provider 205 displayed on the front or back of the card 200. In some examples, the contactless card 200 is not related to a payment card, and may comprise, without limitation, an identification card, a membership card, and a transportation card. In some examples, the payment card may comprise a dual interface contactless payment card. The contactless card 200 may comprise a substrate 210, 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 200 may have physical characteristics compliant with the ID-1 format of the ISO/IEC 7810 standard, and the contactless card may otherwise be compliant with the ISO/IEC 14443 standard. However, it is understood that the contactless card 200 according to

the present disclosure may have different characteristics, and the present disclosure does not require a contactless card to be implemented in a payment card.

[00047] The contactless card 200 may also include identification information 215 displayed on the front and/or back of the card, and a contact pad 220. The contact pad 220 may be configured to establish contact with another communication device, including but not limited to a user device, smart phone, laptop, desktop, or tablet computer. The contactless card 200 may also include processing circuitry, antenna and other components not shown in FIG. 2A. These components may be located behind the contact pad 220 or elsewhere on the substrate 210. The contactless card 200 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 2A).

[00048] As illustrated in FIG. 2B, the contact pad 220 of FIG. 2A may include processing circuitry 225 for storing and processing information, including a microprocessor 230 and a memory 235. It is understood that the processing circuitry 225 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.

[00049] The memory 235 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 200 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-programed many times after leaving the factory. It may also be read many times.

[00050] The memory 235 may be configured to store one or more applets 240, one or more counters 245, and a customer identifier 250. The one or more applets 240 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 applets 240 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 245 may comprise a numeric counter sufficient to store an integer. The customer identifier 250 may comprise a unique alphanumeric identifier assigned to a user of the contactless card 200, and the identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the customer identifier 250 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.

[00051] The processor and memory 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 pad 220 or entirely separate from it, or as further elements in addition to processor 230 and memory 235 elements located within the contact pad 220.

[00052] In some examples, the contactless card 200 may comprise one or more antennas 255. The one or more antennas 255 may be placed within the contactless card 200 and around the processing circuitry 225 of the contact pad 220. For example, the one or more antennas 255 may be integral with the processing circuitry 225 and the one or more antennas 255 may be used with

an external booster coil. As another example, the one or more antennas 255 may be external to the contact pad 220 and the processing circuitry 225.

[00053] In an embodiment, the coil of contactless card 200 may act as the secondary of an air core transformer. The terminal may communicate with the contactless card 200 by cutting power or amplitude modulation. The contactless card 200 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 200 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.

[00054] Figure 3 depicts a method 300 of authenticating data transfer. Figure 3 may reference the same or similar components of system 100, and transmitting device 200 of FIG. 2A and FIG. 2B.

[00055] At block 310, the method 300 may include transmitting, after one or more processors of a transmitting device entering a communication field, a link to a first application comprising instructions for execution on a first device, the link configured to initiate data transfer, the link comprising a near field communication data exchange format uniform resource locator including identifier data and cardholder data. In some examples, the transmittal of the link may occur after dynamically generating the link. In some examples, the transmitting device may enter the communication field of a client device via one or more gestures selected from the group of a tap, swipe, wave, or any combination thereof. In some examples, the user may be identified based on a mobile network operator (MNO) lookup. In other examples, the user may be identified based on one or more cookies associated with prior account logins, e.g., logins to an account associated with the transmitting device, a separate account associated with the user, and/or other accounts.

[00056] The link may comprise a near field communication data exchange format uniform resource locator (NDEF URL). The link may comprise a first set of information and a second set of information. The first set of information may include identifier information. For example, the first set of information may comprise an abstracted user name generated by the processor after entry of the transmitting device into the communication field. For example, the abstracted identification information may be generated for each transaction, such as the dynamically generated URL. Without limitation, the identification information may be generated on the card by combining a unique identifier with one or more variables, such as a counter, one or more cryptographic algorithms, and/or any combination thereof. For example, the one or more cryptographic algorithms may include an encryption technique, such as public or private key encryption, that would also be known by a server for authentication. Without limitation, exemplary symmetric key algorithms may include symmetric key encryption such as DES, Triple DES, or AES. Without limitation, exemplary asymmetric key algorithms may include asymmetric public key encryption, digital signature algorithm, or RSA. For example, the second set of information may include user information, such as cardholder information. In some examples, the second set of information may include cardholder information (e.g., account owner name, account number, expiration date, card verification value).

[00057] At block 320, the method 300 may include authenticating a user associated with the first device by activating one or more actions based on the link. The one or more actions may be configured to request confirmation of a third set of information associated with the data transfer. The third set of information may include at least one selected from the group of a quantity, digital asset, and recipient information. In some examples, at least one action may comprise launching a website configured to identify the user associated with the first device. In other examples, at least

one action may comprise requesting, by the first application, one or more login credentials.

[00058] At block 330, the method 300 may include transmitting one or more requests for confirmation of quantity, digital asset, and recipient data associated with the data transfer. For example, the first application may be configured to receive input indicative of confirmation of the quantity, such as an amount, digital asset, and recipient data, such as recipient, of the peer-to-peer transfer that are associated with the third set of information of block 320.

[00059] At block 340, the method 300 may include receiving one or more notifications that are based on the one or more requests for confirmation of quantity, digital asset, and recipient data associated with the data transfer. The device associated with the transmitting device user, such as the second application of the second device associated with a cardholder, may be configured to receive a notification, including but not limited to a push notification or email, that acts as a second confirmation of the amount, digital asset, and transfer recipient.

[00060] At block 350, the method 300 may include performing one or more login credentials that are responsive to the one or more notifications so as to complete the data transfer. For example, one or more authentication inputs may be received to complete the data transfer. The authentication input may be responsive to the one or more notifications. To confirm the data transfer, the cardholder may select a button to take an action that is responsive to the one or more requests and based on the one or more notifications, such as the requested authentication communication including but an authentication input. Exemplary authentication inputs can include, without limitation, entry of login credentials, account information, security information, biometric information and a combination thereof (e.g., entry of a user name, a password, an account number, a security code, a one-time passcode, an answer to a security question, a fingerprint, a facial scan, a retinal scan, a voice recognition, and logging into an application or website associated with an

account or card-issuing institution). Upon authentication of the login via the received authentication input, the transfer may be confirmed. In addition, the directionality of the data transfer may be reversed. In some examples, by adjusting the directionality of the transfer, such as from transferor to recipient or from recipient to transferor, a corresponding message such as a push notification or email may be generated so as to indicate confirmation of the desired reversed directionality of the transfer. In some examples, the corresponding message may be displayed by the first application and/or second application. In this manner, the peer-to-peer transfer would be for an authenticated user, after the confirmation, since the transfer is to a known recipient.

[00061] In some examples, the peer-to-peer transfer may comprise issuance of credit. The credit may be in accord with one or more spending restrictions. For example, the one or more spending restrictions may include a time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof.

[00062] In some examples, the peer-to-peer transfer may be associated with one or more rewards and/or points. For example, the rewards and/or points may be adjusted for each of the transferor and the transferee, and may be adjusted based on redemption of the credit. For example, the rewards and/or points may be issued and thereby added to a user reward or loyalty point program if the credit is used at a particular merchant, such as a restaurant, and/or at a particular time, such as on the weekends. When the recipient or transferee uses the credit, the transferor may still accrue the rewards and/or points. In some examples, the peer-to-peer transfer may include a plurality of portions. For example, a first portion of the peer-to-peer transfer may be transmitted prior to a second portion of the peer-to-peer transfer. For example, a first portion may comprise one or more rewards, and a second portion may comprise one or more points. Any portion of the transfer may be transmitted at a predetermined time, including but not limited to a day, time, week, month,

and/or any combination thereof.

[00063] In other examples, the peer-to-peer transfer may comprise transfer of one or more digital assets. Without limitation, the digital asset may comprise an image or a document. Without limitation, the format type of the digital asset may include at least one selected from the group of a static image file (such as JPEG, PNG, SVG), a static document file (such as PDF, PSD), an animated file (such as GIF, SWF), and web code (such as HTML, CSS, JavaScript). The one or more digital assets may be identified for transfer. For example, the digital asset may be securely transmitted by launching a website and uploading the identified digital asset for transfer. In another example, the digital asset may be securely transmitted by opening an application or launching an email client in which the identified digital asset may be included as an attachment. In another example, the digital asset may be digital asset may be identified as part of a uniform resource locator (URL) that is transmitted for retrieving the identified digital asset.

[00064] In other examples, the peer-to-peer transfer may comprise a funds transfer, such as a cash transfer. As with the issuance of credit, the funds transfer may be subject to one or more spending restrictions and/or one or more merchants. For example, the funds transfer may be subject to a restriction based on time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof. In some examples, the funds transfer may include a plurality of portions. For example, a first portion of the funds transfer may be transmitted prior to a second portion of the funds transfer. Any portion of the funds transfer may be transmitted at a predetermined time, including but not limited to a day, time, week, month, and/or any combination thereof. In this manner, the funds transfer may be transmitted in aggregate until satisfaction of the entire funds transfer.

[00065] In other examples, the peer-to-peer transfer may comprise issuance of a virtual gift card.

As with the issuance of credit, the virtual gift card may be subject to one or more spending restrictions and/or one or more merchants. For example, the virtual gift card may be subject to a time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof. In some examples, the peer-to-peer transfer may include a plurality of portions associated with various amounts of the virtual gift card. For example, a first portion of the peer-to-peer transfer may be transmitted prior to a second portion of the peer-to-peer transfer. Any portion of the transfer may be transmitted at a predetermined time, including but not limited to a day, time, week, month, and/or any combination thereof.

[00066] Figure 4 depicts a method of initiating and authenticating data transfer according to an exemplary embodiment. Figure 4 may reference the same or similar components of system 100, transmitting device 200 of FIG. 2A and FIG. 2B, and method 300 of FIG. 3. As illustrated in FIG. 4, a peer-to-peer transfer may be initiated by the card entering a communication field of a user device and loading a website.

[00067] At block 405, the method 400 may include the card entering a communication field of the user device, including but not limited to via one or more gestures selected from the group of a tap, swipe, wave, or any combination thereof. This communication may include but not be limited to NFC. At block 410, the method 400 may include loading a website via the NDEF URL to identify the user of the user device after the entry of the card into the communication field of the user device. In some examples, the card may be configured to transmit, after entering the communication field of block 405, a link to a client application of one or more user devices to initiate data transfer. In some examples, the transmittal of the link may occur after dynamically generating the link. In some examples, the client application may be associated with the issuing entity of the transmitting device or card. In other examples, the client application may not be

associated with the issuing entity of the transmitting device or card. For example, the client application may be associated with a third party entity or an entity external to the issuing entity of the transmitting device or card.

[00068] In some examples, the NDEF URL may comprise a domain name and an identifier. For example, the link may include abstracted identification information, including but not limited to an account or user identifier for a cardholder, that is loaded onto the chip at the time of personalization of the card. For example, the URL may be encoded in a NDEF file at card embossing time. The abstracted identification information may be generated for each transaction, such as the dynamically generated URL. Without limitation, the identification information may be generated on the card by combining a unique identifier with one or more variables, such as a counter, one or more cryptographic algorithms, and/or any combination thereof. For example, the one or more cryptographic algorithms may include an encryption technique, such as public or private key encryption, that would also be known by a server for authentication. Without limitation, exemplary symmetric key algorithms may include symmetric key encryption such as DES, Triple DES, or AES. Without limitation, exemplary asymmetric key algorithms may include asymmetric public key encryption, digital signature algorithm, or RSA.

[00069] At block 415, the method 400 may include identifying the user via device fingerprinting, and may be based on, without limitation, at least one selected from the group of device configuration, device memory, device screen size, device operating system version, applications installed, phone carrier provider, third party cookies for websites, phone number tracking through MNO lookup, browser type, browser language, IP address, and/or any combination thereof of a device.

[00070] At block 420, the method may include prompting user login to identify the user if the

website is unable to identify the user via cookies or device fingerprinting. For example, if the website cannot successfully identify the user via at least one selected from the group of operating system, browser type, browser language, IP address, the user may receive a notification, generated by the server, indicative of unsuccessful notification and/or may be prompted by the application to input login information in order to successfully identify the user and that is responsive to the unsuccessful notification.

[00071] At block 425, the method 400 may include loading predetermined information after identifying the user. In some examples, the predetermined information may be any information associated with the cardholder that is already filled out or otherwise provided on the website via being embedded directly in the NDEF URL. The website may be further configured to submit the transfer by selection of a button. Moreover, the website may be further configured to adjust recipient and/or transferor of the data transfer. For example, the directionality of the data transfer may be reversed. In some examples, by adjusting the directionality of the transfer, such as from transferor to recipient or from recipient to transferor, a corresponding message such as a push notification or email may be generated so as to indicate confirmation of the desired reversed directionality of the transfer. In some examples, the corresponding message may be displayed by the first application and/or second application.

[00072] At block 430, the method 400 may include entering quantity and recipient data for the peer-to-peer transfer prior to transfer submission. At block 435, the method 400 may include receiving an email or push notification to confirm the peer-to-peer transfer. For example, the cardholder may be associated with a user device. The application of user device may be configured to receive the notification. At block 440, responsive to receipt of the notification, the notification may be opened or displayed so as to prompt a log in or request biometric input to verify that the

user initiated the transfer. In some examples, the prompt may include a request for one or more authentication inputs. For example, exemplary authentication inputs can include, without limitation, entry of login credentials, account information, security information, biometric information and a combination thereof (e.g., entry of a user name, a password, an account number, a security code, a one-time passcode, an answer to a security question, a fingerprint, a facial scan, a retinal scan, a voice recognition, and logging into an application or website associated with an account or card-issuing institution).

[00073] At block 445, after verification of the one or more authentication inputs, the peer-to-peer transfer between the cardholder and the second user may be scheduled. In some examples, the peer-to-peer transfer may be scheduled at a predetermined time, such as at a predetermined day, time, week, month, and/or year. In other examples, the peer-to-peer transfer may be scheduled instantly. In this manner, the peer-to-peer transfer may be scheduled or placed in queue for transaction without having to identify the person and downloading and signing up for different applications. In addition, the directionality of the data transfer may be reversed. In some examples, by adjusting the directionality of the transfer, such as from transferor to recipient or from recipient to transferor, a corresponding message such as a push notification or email may be generated so as to indicate confirmation of the desired reversed directionality of the transfer. In some examples, the corresponding message may be displayed by the first application and/or second application. In this manner, the peer-to-peer transfer would be for an authenticated user, after the confirmation, since the transfer is to a known recipient.

[00074] In some examples, the peer-to-peer transfer may comprise issuance of credit. The credit may be in accord with one or more spending restrictions. For example, the one or more spending restrictions may include a time limit, amount limit, geographic limit, merchant type, merchant

limit, and/or any combination thereof. In some examples, the issuance of credit may be associated with one or more rewards and/or points. For example, the rewards and/or points may be issued and thereby added to a user reward or loyalty point program if the credit is used at a particular merchant, such as a restaurant, at a particular time, such as on the weekends. For example, the rewards and/or points may be adjusted for each of the transferor and the transferee, and may be adjusted based on redemption of the credit. For example, the rewards and/or points may be issued and thereby added to a user reward or loyalty point program if the credit is used at a particular merchant, such as a restaurant, and/or at a particular time, such as on the weekends. When the recipient or transferee uses the credit, the transferor may still accrue the rewards and/or points.

[00075] In other examples, the peer-to-peer transfer may comprise transfer of one or more digital assets. Without limitation, the digital asset may comprise an image or a document. Without limitation, the format type of the digital asset may include at least one selected from the group of a static image file (such as JPEG, PNG, SVG), a static document file (such as PDF, PSD), an animated file (such as GIF, SWF), and web code (such as HTML, CSS, JavaScript). The one or more digital assets may be identified for transfer. For example, the digital asset may be securely transmitted by launching a website and uploading the identified digital asset for transfer. In another example, the digital asset may be securely transmitted by opening an application or launching an email client in which the identified digital asset may be included as an attachment. In another example, the digital asset may be digital asset may be identified as part of a uniform resource locator (URL) that is transmitted for retrieving the identified digital asset.

[00076] In other examples, the peer-to-peer transfer may comprise a funds transfer, such as a cash transfer. As with the issuance of credit, the funds transfer may be subject to one or more spending restrictions and/or one or more merchants. For example, the funds transfer may be subject

to a restriction based on time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof. In some examples, the funds transfer may include a plurality of portions. For example, a first portion of the funds transfer may be transmitted prior to a second portion of the funds transfer. Any portion of the funds transfer may be transmitted at a predetermined time, including but not limited to a day, time, week, month, and/or any combination thereof. In this manner, the funds transfer may be transmitted in aggregate until satisfaction of the entire funds transfer.

[00077] In other examples, the peer-to-peer transfer may comprise issuance of a virtual gift card. As with the issuance of credit, the virtual gift card may be subject to one or more spending restrictions and/or one or more merchants. For example, the virtual gift card may be subject to time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof. In some examples, the peer-to-peer transfer may include a plurality of portions associated with various amounts of the virtual gift card. For example, a first portion of the peer-to-peer transfer may be transmitted prior to a second portion of the peer-to-peer transfer. Any portion of the transfer may be transmitted at a predetermined time, including but not limited to a day, time, week, month, and/or any combination thereof.

[00078] Figure 5 depicts another method of initiating and authenticating data transfer according to an exemplary embodiment. Figure 5 may reference the same or similar components of system 100, transmitting device 200 of FIG. 2A and FIG. 2B, method 300 of FIG. 3, and method 400 of FIG. 4. As illustrated in FIG. 5, a peer-to-peer transfer may be initiated by the card entering a communication field to a user device and deep linking into an application.

[00079] At block 505, the method may include the card entering a communication field of the user device, including but not limited to via one or more gestures selected from the group of a tap,

swipe, wave, or any combination thereof. This communication may include but not be limited to near-field communication (NFC). At block 510, the method may include launching an application of a user device via the near field communication data exchange format (NDEF URL) after the entry of the card into the communication field of the user device. In some examples, the transmittal of the NDEF URL may occur after dynamically generating the NDEF URL. In some examples, the application may be associated with the issuing entity of the transmitting device. In other examples, the application may not be associated with the issuing entity of the transmitting device. For example, the application may be associated with a third party entity or an entity external to the issuing entity of the transmitting device. At block 515, the method may include deep linking by the application to a peer-to-peer transfer screen including predetermined information. In some examples, the predetermined information may be any information associated with the cardholder that is already filled out or otherwise via being embedded directly in the NDEF URL. In some examples, the application may be configured to, prior to deep linking, prompt the user to log in. In other examples, the application may be configured to, after deep linking, prompt the user to log in. In some examples, the log in, prior to deep linking, may be the same or different as the log in required after deep linking. Moreover, exemplary authentication inputs can include, without limitation, entry of login credentials, account information, security information, biometric information and a combination thereof (e.g., entry of a user name, a password, an account number, a security code, a one-time passcode, an answer to a security question, a fingerprint, a facial scan, a retinal scan, a voice recognition, and logging into an application or website associated with an account or card-issuing institution). At block 520, the method may include entering quantity and recipient data for the peer-to-peer transfer before the transfer is submitted. At block 525, the method may include receiving an email or push notification to confirm the peer-to-peer transfer.

For example, the cardholder may be associated with a user device. The user device or its application may be configured to receive the notification. At block 530, responsive to receipt of the notification, the notification may be opened or displayed so as to prompt the authentication input to verify that the user initiated the transfer. At block 535, after verification, the peer-to-peer transfer between the cardholder and the second user may be scheduled. In some examples, the peer-to-peer transfer may be scheduled at a predetermined time, such as at a predetermined day, time, week, month, and/or year. In other examples, the peer-to-peer transfer may be scheduled instantly. In this manner, the peer-to-peer transfer may be scheduled or placed in queue for transaction without having to identify the person and downloading and signing up for different applications. In addition, the directionality of the data transfer may be reversed. In some examples, by adjusting the directionality of the transfer, such as from transferor to recipient or from recipient to transferor, a corresponding message such as a push notification or email may be generated so as to indicate confirmation of the desired reversed directionality of the transfer. In some examples, the corresponding message may be displayed by the first application and/or second application. In this manner, the peer-to-peer transfer would be for an authenticated user, after the confirmation, since the transfer is to a known recipient.

[00080] In some examples, the peer-to-peer transfer may comprise issuance of credit. The credit may be in accord with one or more spending restrictions. For example, the one or more spending restrictions may include a time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof. In some examples, the issuance of credit may be associated with one or more rewards and/or points. For example, the rewards and/or points may be issued and thereby added to a user reward or loyalty point program if the credit is used at a particular merchant, such as a restaurant, at a particular time, such as on the weekends. For example, the

rewards and/or points may be adjusted for each of the transferor and the transferee, and may be adjusted based on redemption of the credit. For example, the rewards and/or points may be issued and thereby added to a user reward or loyalty point program if the credit is used at a particular merchant, such as a restaurant, and/or at a particular time, such as on the weekends. When the recipient or transferee uses the credit, the transferor may still accrue the rewards and/or points.

[00081] In other examples, the peer-to-peer transfer may comprise transfer of one or more digital assets. Without limitation, the digital asset may comprise an image or a document. Without limitation, the format type of the digital asset may include at least one selected from the group of a static image file (such as JPEG, PNG, SVG), a static document file (such as PDF, PSD), an animated file (such as GIF, SWF), and web code (such as HTML, CSS, JavaScript). The one or more digital assets may be identified for transfer. For example, the digital asset may be securely transmitted by launching a website and uploading the identified digital asset for transfer. In another example, the digital asset may be securely transmitted by opening an application or launching an email client in which the identified digital asset may be included as an attachment. In another example, the digital asset may be digital asset may be identified as part of a uniform resource locator (URL) that is transmitted for retrieving the identified digital asset.

[00082] In other examples, the peer-to-peer transfer may comprise a funds transfer, such as a cash transfer. As with the issuance of credit, the funds transfer may be subject to one or more spending restrictions and/or one or more merchants. For example, the funds transfer may be subject to a restriction based on time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof. In some examples, the funds transfer may include a plurality of portions. For example, a first portion of the funds transfer may be transmitted prior to a second portion of the funds transfer. Any portion of the funds transfer may be transmitted at a

predetermined time, including but not limited to a day, time, week, month, and/or any combination thereof. In this manner, the funds transfer may be transmitted in aggregate until satisfaction of the entire funds transfer.

[00083] In other examples, the peer-to-peer transfer may comprise issuance of a virtual gift card. As with the issuance of credit, the virtual gift card may be subject to one or more spending restrictions and/or one or more merchants. For example, the virtual gift card may be subject to time limit, amount limit, geographic limit, merchant type, merchant limit, and/or any combination thereof. In some examples, the peer-to-peer transfer may include a plurality of portions associated with various amounts of the virtual gift card. For example, a first portion of the peer-to-peer transfer may be transmitted prior to a second portion of the peer-to-peer transfer. Any portion of the transfer may be transmitted at a predetermined time, including but not limited to a day, time, week, month, and/or any combination thereof.

[00084] In this specification, reference is made to types of resource locators, such as a URL, NDEF URL, IRL, URI, and URN. However, it is understood that these references are exemplary, and the present disclosure includes, but is not limited to, the types of resource locators mentioned.

[00085] It is further noted that the systems and methods described herein may be tangibly embodied in one of more physical media, such as, but not limited to, a compact disc (CD), a digital versatile disc (DVD), a floppy disk, a hard drive, read only memory (ROM), random access memory (RAM), as well as other physical media capable of data storage. For example, data storage may include random access memory (RAM) and read only memory (ROM), which may be configured to access and store data and information and computer program instructions. Data storage may also include storage media or other suitable type of memory (e.g., such as, for example, RAM, ROM, programmable read-only memory (PROM), erasable programmable read-

only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), magnetic disks, optical disks, floppy disks, hard disks, removable cartridges, flash drives, any type of tangible and non-transitory storage medium), where the files that comprise an operating system, application programs including, for example, web browser application, email application and/or other applications, and data files may be stored. The data storage of the network-enabled computer systems may include electronic information, files, and documents stored in various ways, including, for example, a flat file, indexed file, hierarchical database, relational database, such as a database created and maintained with software from, for example, Oracle® Corporation, Microsoft® Excel file, Microsoft® Access file, a solid state storage device, which may include a flash array, a hybrid array, or a server-side product, enterprise storage, which may include online or cloud storage, or any other storage mechanism. Moreover, the figures illustrate various components (e.g., servers, computers, processors, etc.) separately. The functions described as being performed at various components may be performed at other components, and the various components may be combined or separated. Other modifications also may be made.

[00086] In the preceding specification, various embodiments have been described with references to the accompanying drawings. It will, however, be evident that various modifications and changes may be made thereto, and additional embodiments may be implemented, without departing from the broader scope of the invention as set forth in the claims that follow. The specification and drawings are accordingly to be regarded as an illustrative rather than restrictive sense.

WE CLAIM:

1. An authenticated data transfer system comprising:

a contactless card comprising a processor and a memory,

wherein, after entering a communication field, the processor is configured to:

dynamically generate a uniform resource locator (URL), wherein the URL comprises:

a first set of information including abstracted identifier information, and

a second set of information including user information; and

and transmit the URL to initiate data transfer; and

wherein the data transfer is completed upon verification of a received response and confirmation of a third set of information associated with the data transfer.

2. The authenticated data transfer system of claim 1, wherein one or more actions, based on the link, are configured to identify a user.

3. The authenticated data transfer system of claim 2, wherein at least one action from the one or more actions comprises launching a website configured to identify the user associated with a first device.

4. The authenticated data transfer system of claim 3, wherein the user associated with the first device is identified by at least one selected from the group of device fingerprinting and a cookie.

5. The authenticated data transfer system of claim 4, wherein login information is requested upon determination of an unsuccessful identification.

6. The authenticated data transfer system of claim 4, wherein the website is configured to display the second set of information and the third set of information.

7. The authenticated data transfer system of claim 6, wherein a notification comprises the one or more responses associated with confirmation of the third set of information.

8. The authenticated data transfer system of claim 7, wherein one or more authentication communications associated with confirmation of the third set of information are performed, the one or more authentication communications including at least one selected from the group of biometric communication and login communication.

9. The authenticated data transfer system of claim 1, wherein the first set of information comprises an abstracted user name generated by the processor after entry of the contactless card into the communication field.

10. The authenticated data transfer system of claim 1, wherein the link comprises a near field communication data exchange format uniform resource locator.

11. The authenticated data transfer system of claim 3, wherein the first device comprises at least one selected from the group of a mobile device, a wearable device, and a kiosk.

12. The authenticated data transfer system of claim 2, wherein at least one action from the one or more actions comprises requesting one or more login credentials.

13. The authenticated data transfer system of claim 12, wherein a deep link to a screen including the second set of information and the third set of information is performed upon submission of the requested one or more login credentials and upon authentication of the one or more login credentials.

14. The authenticated data transfer system of claim 1, wherein the third set of information includes at least one selected from the group of a quantity, digital asset, and recipient information.

15. The authenticated data transfer system of claim 14, wherein a notification comprises the one or more responses associated with confirmation of the third set of information.

16. The authenticated data transfer system of claim 15, wherein one or more authentication communications associated with confirmation of the third set of information are performed, the one or more authentication communications including at least one selected from the group of biometric communication and login communication.

17. The authenticated data transfer system of claim 1, wherein the data transfer is scheduled at a predetermined time.

18. A method of authenticating data transfer, comprising:

dynamically generating, after entry of one or more processors of a transmitting device into a communication field, the link comprising a near field communication data exchange format uniform resource locator including identifier data and user data;

transmitting, to a first application comprising instructions for execution on a first device, the link to initiate data transfer;

authenticating a user associated with the first device by activating one or more actions based on the link;

transmitting one or more requests for confirmation of quantity and recipient data associated with the data transfer;

receiving one or more notifications that are based on the one or more requests for confirmation of quantity and recipient data associated with the data transfer; and

performing one or more login credentials that are responsive to the one or more notifications so as to complete the data transfer.

19. The method of claim 18, wherein at least one action from the one or more actions comprises launching a website configured to identify the user associated with the first device.

20. A computer readable non-transitory medium comprising computer-executable instructions that, when executed by a processor, perform procedures comprising the steps of:

dynamically generating , after entry of a contactless card into a communication field, a link, the link comprising a first set of information and a second set of information, the first set of information including identifier information, the second set of information including user information;

transmitting, to a first application comprising instructions for execution on a first device, the link to initiate data transfer;

identifying a user associated with the first device by activating one or more actions based on the link, the one or more actions configured to request confirmation of a third set of information associated with the data transfer; and

transmitting one or more responses based on authentication of the third set of information so as to complete the data transfer.

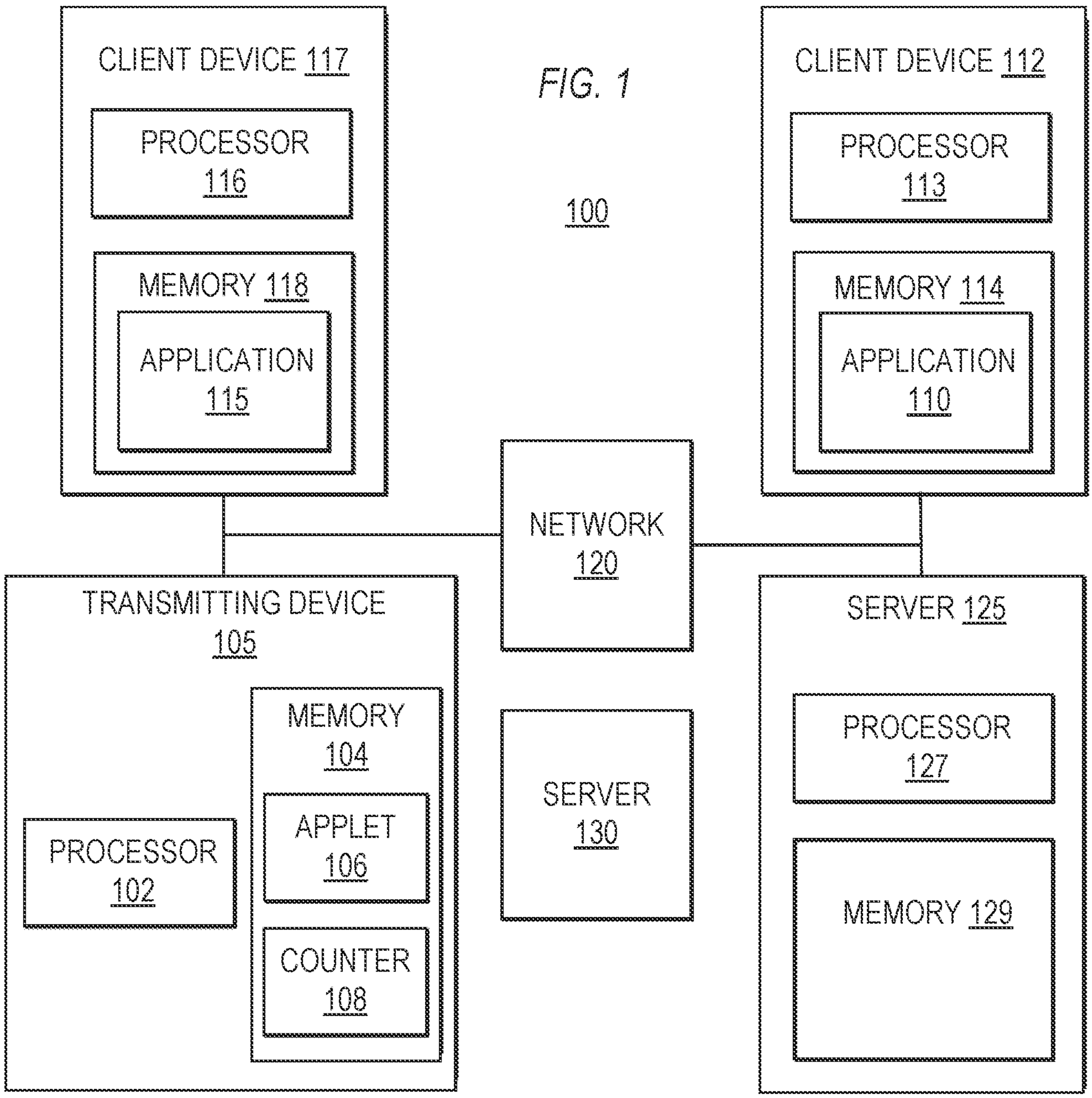

CLIENT DEVICE 117
PROCESSOR 116
MEMORY 118
APPLICATION 115
CLIENT DEVICE 112
PROCESSOR 113
MEMORY 114
APPLICATION 110
100
NETWORK 120
SERVER 130
TRANSMITTING DEVICE 105
PROCESSOR 102
MEMORY 104
APPLET 106
COUNTER 108
SERVER 125
PROCESSOR 127
MEMORY 129

FIG. 1

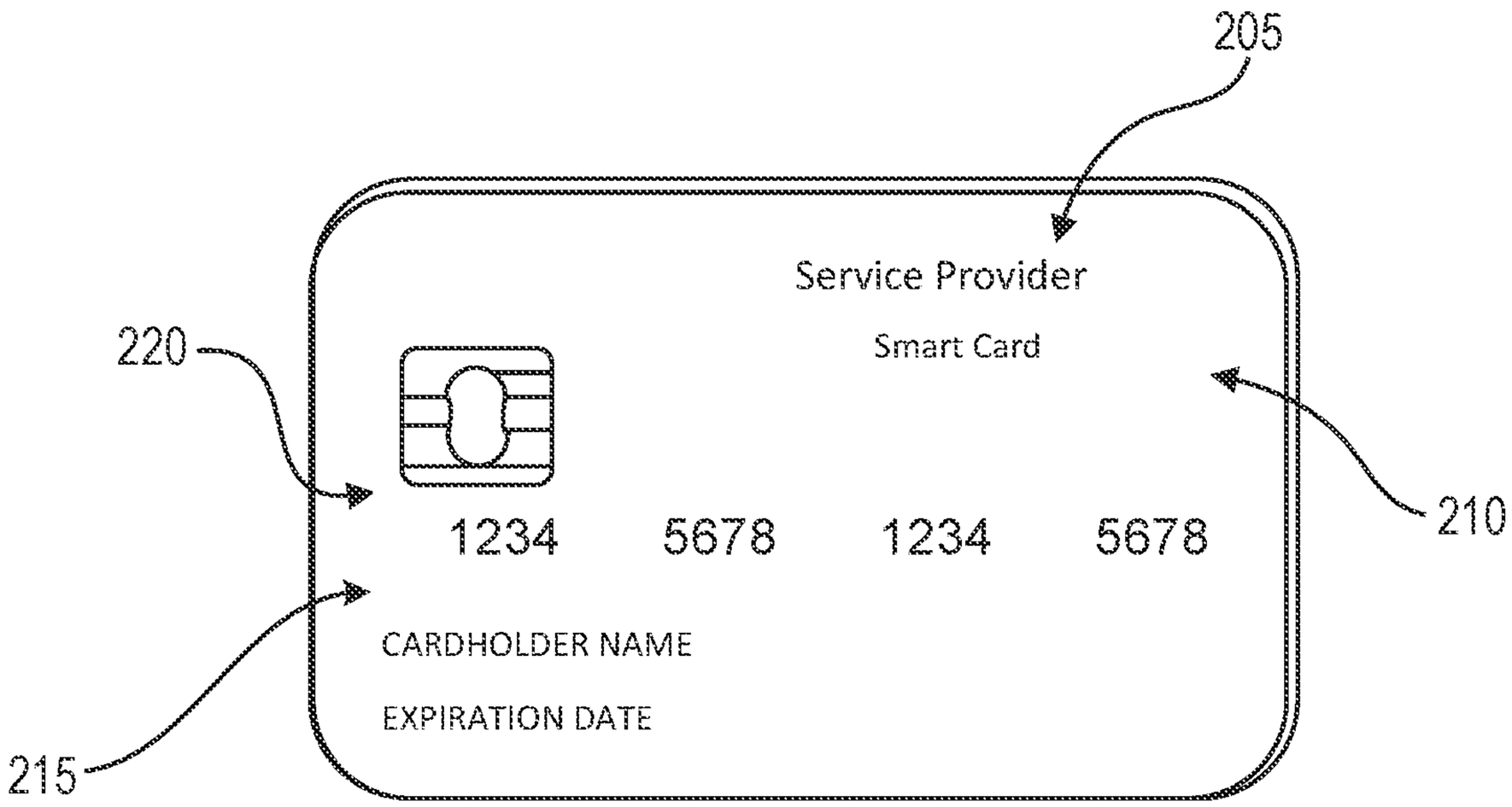

205
Service Provider
Smart Card
220
1234 5678 1234 5678
210
CARDHOLDER NAME
EXPIRATION DATE
215
200

FIG. 2A

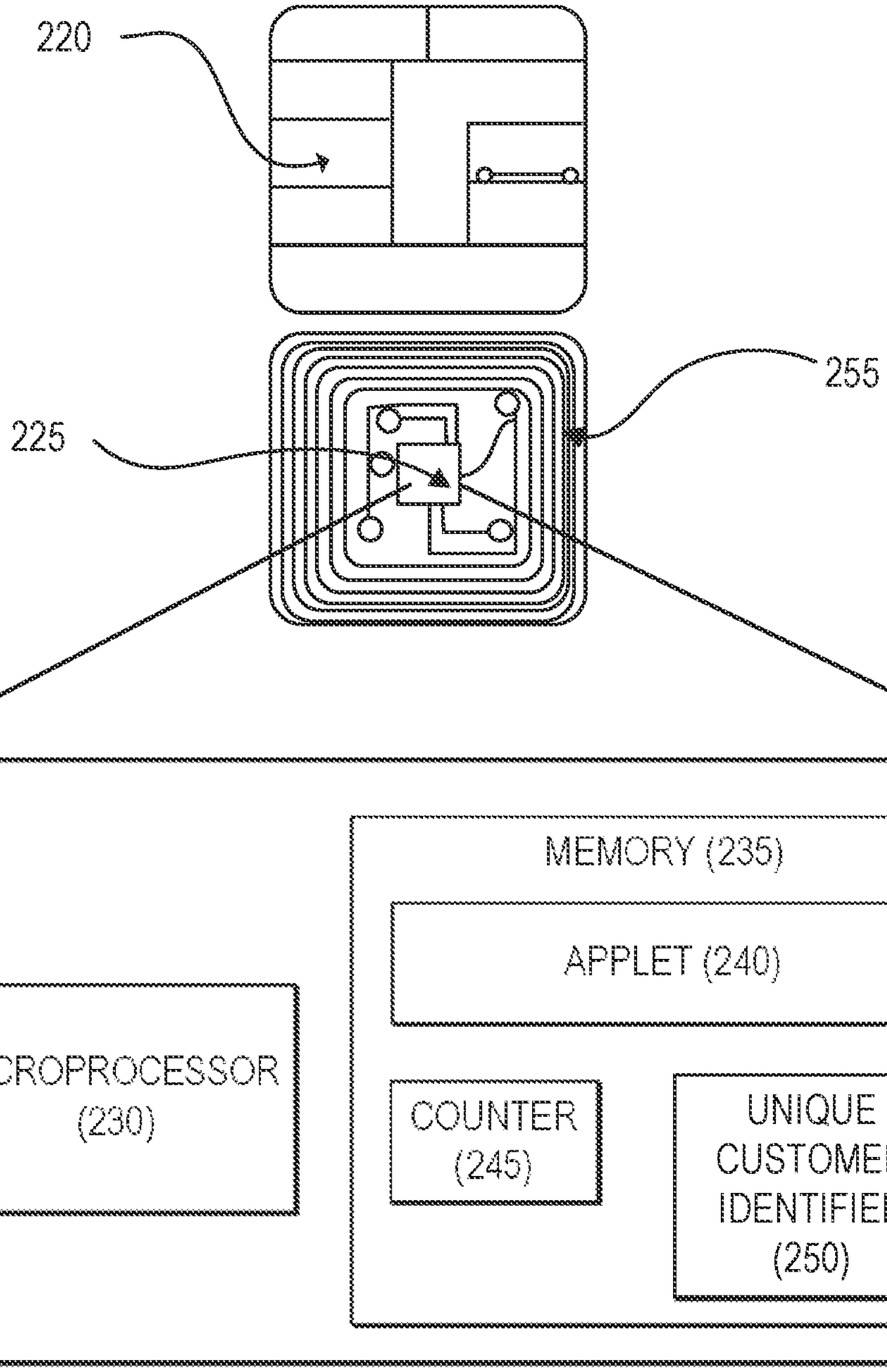

220
225
255
MICROPROCESSOR (230)
MEMORY (235)
APPLET (240)
COUNTER (245)
UNIQUE CUSTOMER IDENTIFIER (250)

FIG. 2B

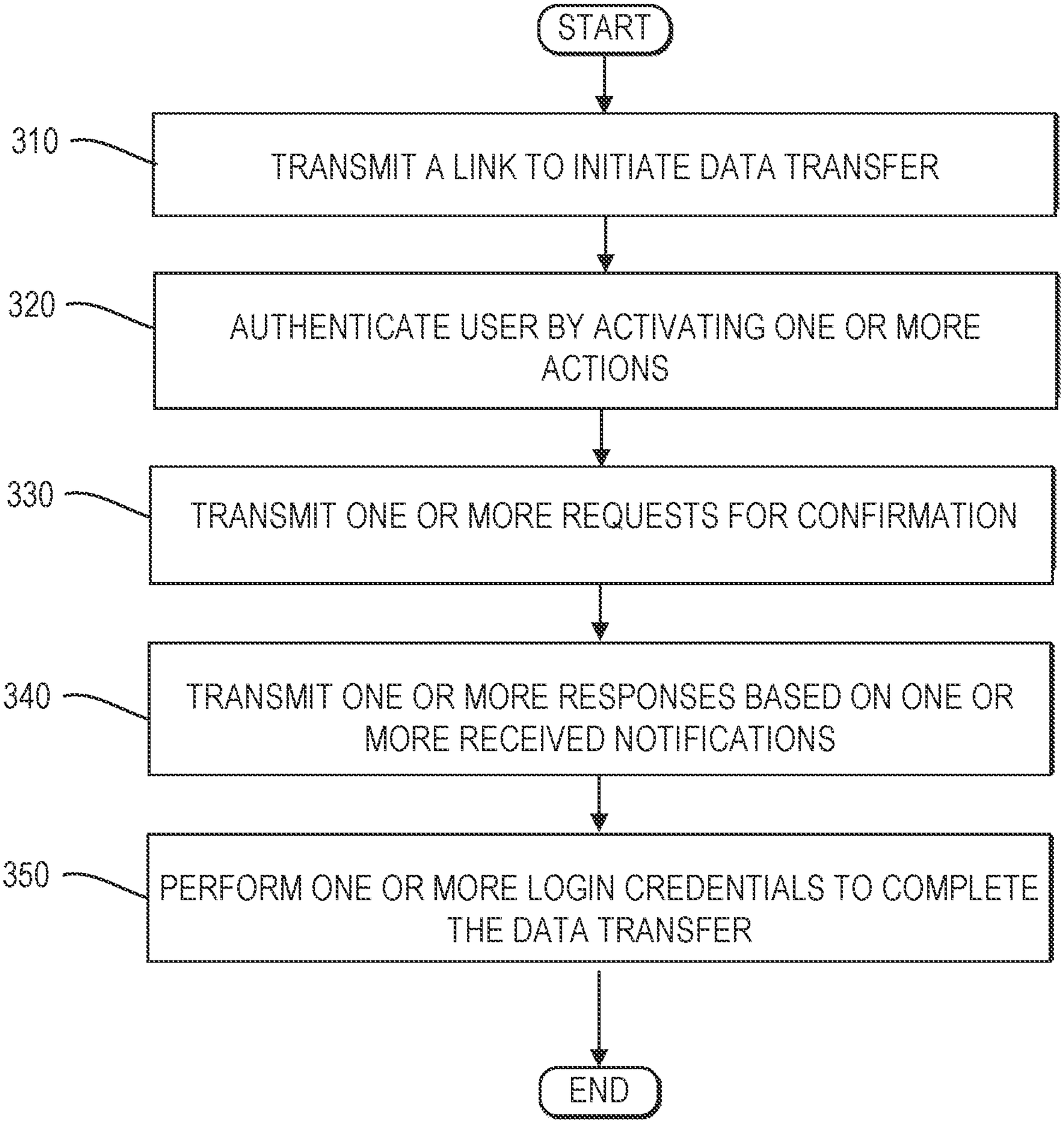

START
310
TRANSMIT A LINK TO INITIATE DATA TRANSFER
320
AUTHENTICATE USER BY ACTIVATING ONE OR MORE ACTIONS
330
TRANSMIT ONE OR MORE REQUESTS FOR CONFIRMATION
340
TRANSMIT ONE OR MORE RESPONSES BASED ON ONE OR MORE RECEIVED NOTIFICATIONS
350
PERFORM ONE OR MORE LOGIN CREDENTIALS TO COMPLETE THE DATA TRANSFER
END
300

FIG. 3

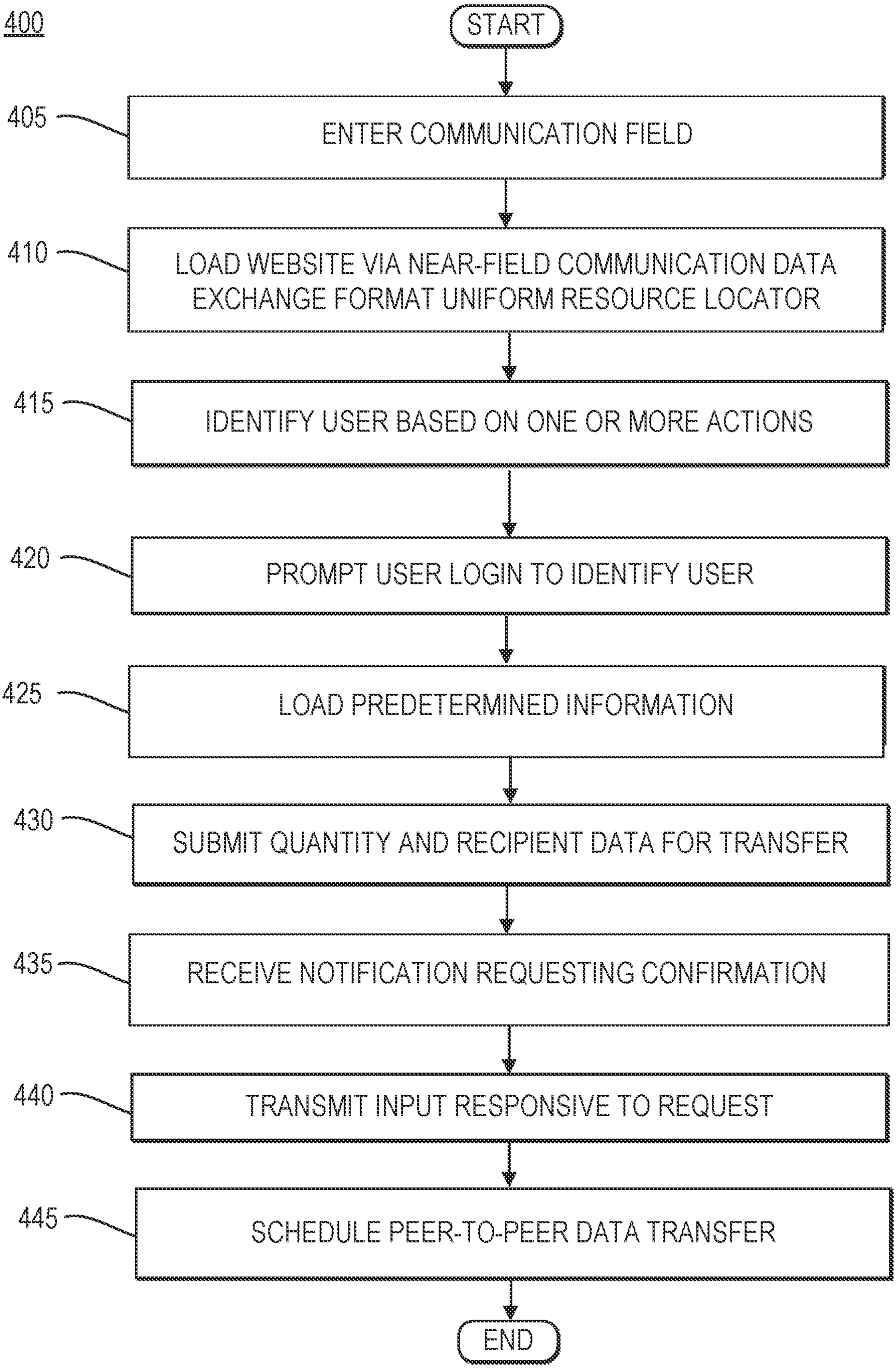

400
START
405
ENTER COMMUNICATION FIELD
410
LOAD WEBSITE VIA NEAR-FIELD COMMUNICATION DATA EXCHANGE FORMAT UNIFORM RESOURCE LOCATOR
415
IDENTIFY USER BASED ON ONE OR MORE ACTIONS
420
PROMPT USER LOGIN TO IDENTIFY USER
425
LOAD PREDETERMINED INFORMATION
430
SUBMIT QUANTITY AND RECIPIENT DATA FOR TRANSFER
435
RECEIVE NOTIFICATION REQUESTING CONFIRMATION
440
TRANSMIT INPUT RESPONSIVE TO REQUEST
445
SCHEDULE PEER-TO-PEER DATA TRANSFER
END

FIG. 4

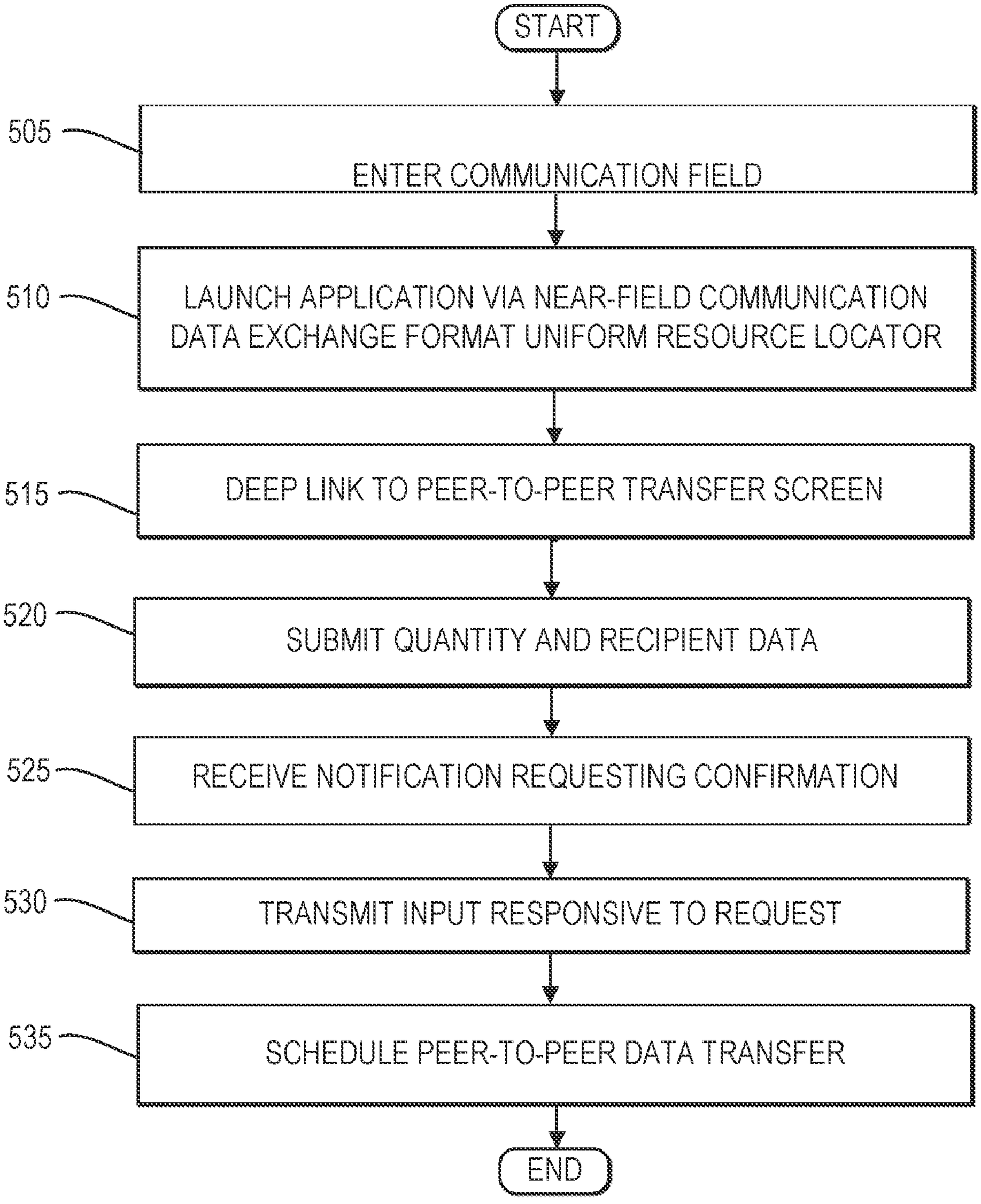

START
505
ENTER COMMUNICATION FIELD
510
LAUNCH APPLICATION VIA NEAR-FIELD COMMUNICATION DATA EXCHANGE FORMAT UNIFORM RESOURCE LOCATOR
515
DEEP LINK TO PEER-TO-PEER TRANSFER SCREEN
520
SUBMIT QUANTITY AND RECIPIENT DATA
525
RECEIVE NOTIFICATION REQUESTING CONFIRMATION
530
TRANSMIT INPUT RESPONSIVE TO REQUEST
535
SCHEDULE PEER-TO-PEER DATA TRANSFER
END

FIG. 5