

**ACCURATE IMAGES IN GRAPHICAL USER INTERFACES TO ENABLE DATA
TRANSFER**

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. Patent Application Serial No. 16/863,401, entitled “ACCURATE IMAGES IN GRAPHICAL USER INTERFACES TO ENABLE DATA TRANSFER” filed on April 30, 2020. The contents of the aforementioned patent application are incorporated herein by reference in their entirety.

TECHNICAL FIELD

Embodiments herein generally relate to computer software, and more specifically, to providing accurate images in graphical user interfaces to enable data transfer.

BACKGROUND

[0001] Cardholders (e.g., credit card holders, bank card holders, etc.) often use computer-based applications to perform various account-related activities. Often, the user may be required to tap the card to a computing device to enable data transfer. However, due to device differences, card differences, and any other factors, different orientations and/or placements of the card relative to the computing device may be required to enable data transfer.

SUMMARY

[0002] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for providing accurate images of contactless cards in graphical user interfaces on computing devices. According to one example, an application executing on a processor may receive authentication credentials for an account. The application may determine a first contactless payment card associated with the account and a card manufacturer identifier (CMID) of the first contactless payment card. The application may receive, from a digital asset management system based on the CMID, a plurality of images of the first payment card and a plurality of metadata attributes of the first contactless payment card. The application may determine, based on the plurality of metadata attributes of the first contactless payment card and a plurality of attributes of the mobile device, a first orientation of the first contactless payment card to enable near-field communication (NFC) data transfer between the first contactless payment card and the mobile device. The application may select a first image of the plurality of images depicting the first contactless payment card according to the first orientation. The application may generate a graphical user interface (GUI) depicting the first image of the plurality of images of the first contactless payment card and an indication specifying to tap the first contactless payment card to the mobile device according to the first orientation and display the GUI on a display.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Figures 1A-1B illustrate an example contactless card.

[0004] Figures 2A-2C illustrate embodiments of a system for providing accurate images of contactless cards in graphical user interfaces to enable data transfer.

[0005] Figures 3A-3B illustrate example graphical user interfaces including accurate images of contactless cards to enable data transfer with computing devices.

[0006] Figures 4A-4B illustrate example graphical user interfaces including accurate images of contactless cards to enable data transfer with computing devices.

[0007] Figures 5A-5B illustrate example graphical user interfaces including accurate images of contactless cards to enable data transfer with computing devices.

[0008] Figure 6 illustrates an embodiment of a first logic flow.

[0009] Figure 7 illustrates an embodiment of a second logic flow.

[0010] Figure 8 illustrates an embodiment of a computing architecture.

DETAILED DESCRIPTION

[0011] Embodiments disclosed herein provide accurate images of payment cards for use in graphical user interfaces (GUIs) on computing devices based at least in part on metadata of the payment cards. The accurate images of the payment cards in the GUIs may assist users in orienting the payment card relative to the computing device in a manner that enables data transfer between the payment card and the computing device. Generally, when a payment card is manufactured, the payment card may be assigned a unique card manufacture identifier (CMID) the uniquely identifies the card. Furthermore, one or more images of the card (and/or one or more base images of a type of the card) may be stored in a digital asset management (DAM) system along with metadata attributes describing the card.

[0012] When a user logs in to their account in an application, the CMID of one or more cards associated with the account may be determined by the application. The application may then use the CMID to query the DAM system to receive the one or more images of the card and the metadata attributes of the card. The application may further determine one or more attributes of the computing device on which the application is executing. Based on the card attributes and/or device attributes, the application may determine an orientation of the card (e.g., front-facing) that would result in optimal data transfer between the card and the device (relative to other orientations of the card). The application may then select at least one image of the card received from the DAM system that depicts the card in the determined orientation (e.g., front-facing). The application may then generate a GUI using the selected image of the card. The GUI may further depict the selected image of the card being brought within communications range of the computing device (e.g., tapping the card while front-facing to the screen of the computing device). Doing so may facilitate data transfer between the card and computing device without requiring multiple attempts to initiate data transfer.

[0013] Furthermore, when base images of the card are selected, additional data may be overlaid on the base images to make the base image appear more similar to the actual physical card. For example, the account holder's name, the card number, expiration date, and card verification value (CVV) may be overlaid on the base image of the card. One or more logos may also be overlaid on the card based on the logos depicted on the physical card. Further still, other assistive elements may be depicted in the GUI. For example, dashed guidelines may depict an outline of where the card should be placed relative to the computing device.

[0014] As another example, a camera of the computing device may be used to identify different features of the physical card in possession of the user. For example, the camera may capture an image of the physical card and the application may analyze the captured image to perform additional features. In one embodiment, a color of the physical card depicted in the image may be used to determine if the user is using the correct card for a requested operation in the application. For example, if the user is attempting to transfer funds using a first card having metadata attributes indicating the card is red, the image may depict a blue card. Based on the different colors, the application may inform the user that the incorrect card is being used. As another example, a graphical marker may be written on the card. In some embodiments, the graphical marker may not be visible to the human eye but may be detected by the camera. The graphical marker may be used to retrieve different attributes of the card. For example, the graphical marker may be a matrix barcode that is directed to a uniform resource locator (URL) for the card in the DAM system. Doing so may allow the application to determine attributes of the card, determine whether the user is using the correct card, etc.

[0015] Advantageously, embodiments disclosed herein improve graphical user interfaces by providing accurate images of specific cards in the GUIs. The use of accurate images of the card may result in an optimal orientation of the card relative to the computing device, thereby enabling faster, more reliable, wireless data transfer between the card and the device relative to other orientations of the card/device. Similarly, using accurate images to result in the optimal orientation of the card relative to the computing device may enable data transfer that would not be enabled with other orientations (e.g., where data transfer is restricted due to one or more other orientations). Doing so may improve performance of the computing device by requiring fewer power and other resources when communicating with the card.

[0016] With general reference to notations and nomenclature used herein, one or more portions of the detailed description which follows may be presented in terms of program procedures executed on a computer or network of computers. These procedural descriptions and representations are used by those skilled in the art to most effectively convey the substances of their work to others skilled in the art. A procedure is here, and generally, conceived to be a self-

consistent sequence of operations leading to a desired result. These operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to those quantities.

[0017] Further, these manipulations are often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. However, no such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein that form part of one or more embodiments. Rather, these operations are machine operations. Useful machines for performing operations of various embodiments include digital computers as selectively activated or configured by a computer program stored within that is written in accordance with the teachings herein, and/or include apparatus specially constructed for the required purpose or a digital computer. Various embodiments also relate to apparatus or systems for performing these operations. These apparatuses may be specially constructed for the required purpose. The required structure for a variety of these machines will be apparent from the description given.

[0018] Reference is now made to the drawings, wherein like reference numerals are used to refer to like elements throughout. In the following description, for the purpose of explanation, numerous specific details are set forth in order to provide a thorough understanding thereof. It may be evident, however, that the novel embodiments can be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to facilitate a description thereof. The intention is to cover all modification, equivalents, and alternatives within the scope of the claims.

[0019] Figure 1A illustrates a contactless card 101, which may comprise a payment card, such as a credit card, debit card, and/or a gift card. As shown, the contactless card 101 may be issued by a service provider 109 displayed on the front or back of the card 101. In some examples, the contactless card 101 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 101 may comprise a substrate 110, 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 101 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 101 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.

[0020] The contactless card 101 may also include identification information 115 displayed on the front and/or back of the card, and a contact pad 120. The contact pad 120 may be configured to establish contact with another communication device, such as a user device, smartphone, laptop, desktop, or tablet computer. The contactless card 101 may also include processing circuitry, antenna and other components not shown in FIG. 1A. These components may be located behind the contact pad 120 or elsewhere on the substrate 110. The contactless card 101 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 1A).

[0021] As illustrated in FIG. 1B, the contact pad 120 of contactless card 101 may include processing circuitry 125 for storing and processing information, including a microprocessor 130 and the memory 102. It is understood that the processing circuitry 125 may contain additional components, including 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.

[0022] The memory 102 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 101 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. A read/write memory may also be read many times after leaving the factory.

[0023] The memory 102 may be configured to store one or more applets 103, a private key 104, encrypted data 105, one or more customer (or user) identifiers (IDs) 107, and a card manufacture ID (CMID) 108. In some embodiments, the CMID 108 is not stored in the memory 102. The one or more applets 103 may comprise one or more software applications configured to execute on one or more contactless cards, such as a Java® Card applet. However, it is understood that applets 103 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 customer ID 107 may comprise a unique alphanumeric identifier assigned to a user of the contactless card 101, and the

identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the customer ID 107 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. In some embodiments, the applet 103 may use the customer ID 107 as input to a cryptographic algorithm with the private key 104 to generate encrypted data 105.

[0024] 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 120 or entirely separate from it, or as further elements in addition to processor 130 and memory 102 elements located within the contact pad 120.

[0025] In some examples, the contactless card 101 may comprise one or more antennas 155. The one or more antennas 155 may be placed within the contactless card 101 and around the processing circuitry 125 of the contact pad 120. For example, the one or more antennas 155 may be integral with the processing circuitry 125 and the one or more antennas 155 may be used with an external booster coil. As another example, the one or more antennas 155 may be external to the contact pad 120 and the processing circuitry 125.

[0026] In an embodiment, the coil of contactless card 101 may act as the secondary of an air core transformer. The terminal may communicate with the contactless card 101 by cutting power or amplitude modulation. The contactless card 101 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 101 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. More generally, using the antennas 155, processing circuitry 125, and/or the memory 102, the contactless card 101 provides a communications interface to communicate via NFC, Bluetooth, and/or Wi-Fi communications.

[0027] As explained above, contactless cards 101 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 (e.g., the card reader 218 of the device 210 of Figures 2A-2C), and produce an NDEF message that comprises a cryptographically secure OTP encoded as an NDEF text tag.

[0028] In some embodiments, the contactless card 101 may include one or more locations that are associated with optimal placement relative to a card reader to enable data transfer. In some

embodiments, the one or more optimal locations may include the processing circuitry 125, the contact pad 120, the antenna 155, the coil, or some other location on the surface of the contactless card 101. For example, returning to Figure 1A, the location 111 may be one optimal location for tapping the contactless card 101 to a card reader. However, because different materials may be used to produce a given contactless card 101, the location 111 may differ across different contactless cards 101. In some embodiments, the location 111 may be stored as a metadata attribute of a contactless card 101 (or a type of contactless card), e.g., in the DAM 225 of Figure 2A. As shown, the contactless card 101 may further include a graphical marker 112. In some embodiments, the graphical marker 112 is not visible to the human eye but may be detected by a camera or other scanning device. The marker 112 may include any type of marker, such as a matrix barcode, matrix code, fiducial marker, and the like. The marker 112 may be used to encode metadata attributes of the contactless card 101, such as card type, one or more optimal locations 111, materials used to manufacture the contactless card 101, and the like.

[0029] Figure 2A depicts a schematic of an exemplary system 200, consistent with disclosed embodiments. As shown, the system 200 includes one or more contactless cards 101, one or more mobile computing devices 210, and a server 220. As stated, the contactless cards 101 may comprise one or more communications interfaces, such as a radio frequency identification (RFID) chip, configured to communicate with the devices 210 via NFC, the EMV standard, or other short-range protocols in wireless communication. Although NFC is used as an example communications protocol, the disclosure is equally applicable to other types of wireless communications, such as the EMV standard, Bluetooth, and/or Wi-Fi. The mobile devices 210 are representative of any type of network-enabled computing devices, such as smartphones, tablet computers, wearable devices, laptops, portable gaming devices, and the like. The server 220 is representative of any type of computing device, such as a server, workstation, compute cluster, cloud computing platform, virtualized computing system, and the like.

[0030] The computing device 210 and the server may be under the control of an operating system (OS) (not pictured). Example operating systems include the Android® OS, iOS®, macOS®, Linux®, and Windows® operating systems. As shown, a memory 211 of the computing device 210 includes an account application 213. The account application 213 allows users to perform various account-related operations, such as viewing account balances, purchasing items, processing payments, account selection, balance transfer, activation of contactless cards 101, and generating virtual account numbers associated with a contactless card 101. In some embodiments, a user may authenticate using authentication credentials to access certain features of the account application 213. For example, the authentication credentials may include a username and password, biometric credentials (e.g., fingerprints, Face ID, etc.), and the like.

[0031] As shown, a memory 222 of the server 220 includes an authentication application 223, a data store of account data 224, and a digital asset management (DAM) system 225. The authentication application 223 may interface with the account application 213. For example, as described in greater detail below, the authentication application 223 may authenticate encrypted data 105 generated by the contactless card 101 based on copies of the private key 104 and the customer ID 107 that are locally accessible to the server 220. The account data 224 generally stores account-related information for each of a plurality of users. For example, the account data 224 may indicate one or more contactless cards 101 associated with each account and a CMID of each card 101. The DAM system 225 stores information describing different assets, such as the contactless cards 101.

[0032] As stated, when a contactless card 101 is manufactured, the contactless card 101 may be assigned a CMID 108 which uniquely identifies the card. The CMID 108 may be stored in the user profile of the associated cardholder in the account data 224 and/or the DAM system 225. Furthermore, one or more images 231 of the card 101 may be stored in the DAM system 225 with metadata attributes 232 describing the card 101 (e.g., materials used to manufacture the card, one or more locations associated with optimal wireless data transfer, physical arrangement of the components of the contactless card depicted in Figs. 1A-1B, one or more known limitations of the card (e.g., that the card 101 cannot be read when the back side of the card 101 is tapped to a device 210), etc.). The images of a given card 101 may be generic to a type of card (e.g., one or more base images of a given type of card, where a plurality of different types of cards may exist) and/or images of the actual physical card 101 itself.

[0033] As stated, users of the account application 213 may generally attempt to perform any number of operations. Often, wireless data transfer between the contactless card 101 and the device 210 may be required to authorize an operation, such as generating a one-time-use virtual account number for the contactless card 101. However, users may often use an improper orientation of the card 101 and the device 210, which may restrict or otherwise slow data transfer between the card 101 and the device 210. For example, a user may attempt to tap the card 101 to the screen of the device 210. However, on some devices and/or for some cards 101, NFC data transfer cannot occur when the card 101 is on the screen of the device 210. Instead, in some embodiments, the card 101 must be tapped to the back of the device 210 to enable NFC data transfer. Advantageously, however, the account application 213 may generate GUIs which depict an exact image of the card 101 being tapped to the device 210 in the proper orientation and/or placement. The GUIs of the account application 213 may further provide visual markers that assist users in proper placement and orientation of the card 101 relative to the device 210. Doing so may improve data transfer capabilities and/or data transfer rates between the card 101 and device 210.

[0034] To generate the GUIs including accurate images of the card 101, the account application 213 may receive the CMID 108 of the card 101. For example, the account application 213 may receive the CMID 108 stored in the memory of the card 101 via wireless data transfer. In another example, the account application 213 may receive the CMID 108 from the account data 224 of the server 220 when the user provides authentication credentials that are authorized by the server 220. In another example, the account application 213 may store a local instance (not pictured) of the account data 224 for the user account and receive the CMID 108 for each card associated with the account from the local instance of the account data 224. The CMID 108 may generally identify a type, or style of the card (e.g., a metallic card of a first card type). In some examples, the user may tap the card 101 to the device 210 prior to logging into an account via the account application 213. In such examples, the CMID 108 may be received directly from the card and/or received from the account data 224 of the server 220.

[0035] Regardless of the technique used to receive the CMID 108, the account application 213 may use the CMID 108 to query the DAM system 225. Figure 2B depicts an embodiment where the DAM system 225 returns one or more images 231 and card metadata 232 associated with the CMID 108 of the card 101. As depicted in Figure 2C, the account application 213 may determine an optimal orientation 233 of the contactless card 101 for depiction in a GUI to assist the user. The optimal orientation 233 may be based on the card metadata 232 and device attributes 214 of the device 210. For example, the device attributes 214 of the device 210 may specify that the device 210 requires the contactless card 101 to be tapped to the screen of the device 210 to enable NFC data transfer. The device attributes 214 and/or the card metadata 232 may further specify that the card 101 must be front-side up when tapped to a given device 210. As such, the account application 213 may determine that the optimal orientation 233 of the card 101 is front-side up (e.g., the front surface of the card depicted in Figure 1A). The account application 213 may then select an image 231 depicting the card in a front-side up orientation. The account application 213 may further select the image 231 that depicts the card in a rotated orientation, such that one or more reference markers of the card 101 (e.g., the contact pad 120, the point 111, etc.) align with one or more markers of the device attributes 214. The images 231 may generally include a plurality of different images of a given card 101 from a plurality of different angles and/or orientations. Furthermore, the images 231 may include specific visual elements of a contactless card 101, such as logos, colored templates, and the like.

[0036] More generally, the card metadata 232 may generally include any type of metadata attribute for a given contactless card 101. The card metadata 232 may be different for different cards, as different materials may be used to construct different types of cards. Furthermore, because of the way a card is constructed (and/or the components used to construct the card), the

card 101 may favor one side (e.g., the left side, right side, front side, back side, etc.). Therefore, the card metadata 232 may specify one or more materials used to manufacture the contactless card 101 (e.g. the substrate 110), the components used in the contactless card 101 (e.g., the antenna 155, circuitry 125, and other elements depicted in Figures 1A-1B), placement of the components (e.g., a location of the antenna 155 of the contactless card 101, a location of the processing circuitry 125 of the contactless card 101, etc.), one or more colors on the surface of the contactless card 101, one or more logos or other artwork on the surface of the contactless card 101, and one or more locations 111 (or points) on the surface of the contactless card 101 that are optimal locations for data transfer. As additional examples, the card metadata 232 may specify a default orientation for data transfer. The orientation may be vertical and/or horizontal. Additionally and/or alternatively the orientation may be face-up or face-down. Doing so may allow the account application 213 to determine an optimal orientation and location for tapping the contactless card 101 to a device 210.

[0037] The device attributes 214 may include any type of metadata attribute for a type of device 210. Often, different devices 210 have different properties which require different placement locations to enable wireless data transfers with the contactless card 101. Therefore, the device attributes 214 may specify a location of an NFC antenna of the card reader 218 of the device 210, a location on the surface of the device 210 where the contactless card 101 is to be tapped to enable NFC data transfer (e.g., on the front surface, on the rear surface, on the display, etc.). The device attributes 214 may further specify default orientations for the contactless card 101 (e.g., face-up and/or face-down, vertical and/or horizontal, etc.). Doing so may allow the account application 213 to determine an optimal orientation and location for tapping the contactless card 101 to a specific device 210.

[0038] In some embodiments, the image 231 may be a base image of a specific type of card, rather than an image of the actual physical card 101 itself. To provide more accurate images, the account application 213 may overlay data on the selected image 231. For example, the account application 213 may overlay the user's name, the account number of the card 101, the expiration date of the card 101, and/or the CVV of the card 101. In addition and/or alternatively, the account application 213 may overlay an image including a logo depicted on the card 101. The image with the logo may be received from the DAM 225 and may be associated with the CMID 108 of the contactless card 101. Doing so may provide more accurate images of the card 101, as the logos on a given type of card may change over time.

[0039] As shown, in Figure 2A, the device 210 includes a camera 219. The camera 219 may be a front-facing and/or rear-facing camera. The camera 219 may capture images when an instructional GUI is being depicted to assist the user in tapping the contactless card 101 to the

device 210. For example, the front-facing camera 219 may capture an image and determine that the card 101 is covering the camera 219 based on analysis of the image performed by the account application 213 using image recognition and/or computer vision algorithms. The account application 213 may further determine that data transfer has not started between the card 101 and the device 210. Therefore, the account application 213 may generate an audio and/or visual alert indicating to change the orientation of the contactless card 101. For example, the account application 213 may select a different image 231 of the card 101 that depicts the card 101 according to a different orientation. The account application 213 may then output the selected image in the GUI to assist the user.

[0040] As another example, the account application 213 may analyze an image captured by the camera 219 and determine that a blue contactless card 101 is depicted in the image. However, the account application 213 may determine that the blue color of the contactless card 101 does not match a known red color of the card 101 being used to perform an operation (e.g., to process a transfer of funds, generate a virtual account number, etc.). In one embodiment, the red color of the card 101 may be specified as card metadata 232 received from the DAM 225. In addition and/or alternatively, the account application 213 may determine that the color of the card 101 should be red based on the card images 231 received from the DAM 225. If the color of the card in the image captured by the camera 219 does not match the known color of the card 101, the account application 213 may generate and output a notification specifying that the correct card is not being used. In some embodiments, detection of a different card 101 may indicate attempted fraud. For example, when detecting the blue card, the account application 213 may identify fraudulent activity, and generate a fraud alert.

[0041] In another example, the account application 213 may detect the marker 112 in an image captured by the camera 219. Doing so may allow the account application 213 to determine whether the correct card is being presented. Doing so may also allow the account application 213 to determine one or more attributes of the contactless card 101. For example, the account application 213 may decode the marker 112 to determine one or more elements of card metadata 232 (e.g., a color of the card, a type of the card, a material used to manufacture the card, etc.). As another example, the marker 112 may encode (or otherwise be associated with) a URL directed to a record for the contactless card 101 in the DAM system 225. The account application 213 may therefore receive one or more images 231 and/or elements of card metadata 232 from the DAM system 225 (e.g., by accessing the decoded URL).

[0042] In some embodiments, the account application 213 may be opened responsive to a tap of the contactless card 101 to the device 210 (e.g., when the user is interacting with a different application). When the card 101 is tapped to the device 210, the contactless card 101 is brought

sufficiently close to the card reader 218 of the computing device 210. Doing so enables data transfer (e.g., NFC data transfer, Bluetooth data transfer, etc.) between the communications interface (e.g., at least the antenna and coil of Figure 1B) of the contactless card 101 and the card reader 218 of the computing device 210. The applet 103 of the contactless card 101 may then generate and transmit encrypted data 105 to the computing device 210. For example, the applet 103 of the contactless card 101 may use a cryptographic algorithm to generate a cryptographic payload of encrypted data 105 based at least in part on the private key 104 stored in the memory 102 of the contactless card 101. In such an embodiment, the private key 104 and some other piece of data (e.g., a customer identifier, an account identifier, etc.) may be provided as the input to the cryptographic algorithm, which outputs the encrypted data 105. Generally, the applet 103 may use any type of cryptographic algorithm and/or system to generate the encrypted data 105, and the use of a specific cryptographic algorithm as an example herein should not be considered limiting of the disclosure. In some embodiments, the applet 103 may perform encryption using a key diversification technique to generate the encrypted data 105. Examples of key diversification techniques are described in United States Patent Application 16/205,219, filed November 29, 2018. The aforementioned patent application is incorporated by reference herein in its entirety.

[0043] Once generated, the applet 103 may transmit the encrypted data 105 to the account application 213 of the computing device 210, e.g., via NFC. The account application 213 may transmit the encrypted data 105 to the authentication application 223 of the server 220. Once received, the authentication application 223 may authenticate the encrypted data 105. For example, the authentication application 223 may attempt to decrypt the encrypted data 105 using a cryptographic function and copy of the private key 104 stored by the server 220. The private key 104 may be identical to the private key 104 stored in the memory 102 of the contactless card 101, where each contactless card 101 is manufactured to include a unique private key 104 (and the server 220 stores a corresponding copy of each unique private key 104). Therefore, the authentication application 223 may successfully decrypt the encrypted data 105, thereby verifying the encrypted data 105. Although the private key 104 is depicted as being stored in the memory 222, the private key 104 may be stored elsewhere, such as in a secure element and/or a hardware security module (HSM). In such embodiments, the secure element and/or the HSM may decrypt the encrypted data 105 using the private key 104 and a cryptographic function.

[0044] For example, as stated, the customer ID 107 may be used to generate the encrypted data 105. In such an example, the authentication application 223 may decrypt the encrypted data 105 using the private key 104 of the server 220. If the result of the decryption yields the customer identifier associated with the account in the account data 224, the authentication application 223 verifies the encrypted data 105. If the authentication application 223 is unable to decrypt the

encrypted data to yield the expected result (e.g., the customer identifier of the primary account associated with the contactless card 101), the authentication application 223 does not validate the encrypted data 105. Upon verification of the encrypted data 105, the authentication application 223 may determine the CMID 108 of the contactless card 101 from the account data 224. The authentication application 223 may then instruct the DAM 225 to send the card images 231 and metadata 232 corresponding to the determined CMID 108 to the account application 213.

[0045] Figure 3A illustrates an example GUI 300 generated by the account application 213 executing on a device 210. As stated, in some embodiments, a user may provide authentication credentials prior to the GUI 300 being generated by the account application 213. Furthermore, the user may specify to perform a type of operation prior to the GUI 300 being generated (e.g., balance transfer, virtual account number generation, etc.). As shown, the GUI 300 depicts an example mobile device 301. The GUI 300 further depicts an optimal placement location 302 (in dashed lines) for placing a contactless card 101 to enable data transfer. The placement location 302 may generally be based on the device attributes 214 of the device 210 and/or the card metadata 232 of the contactless card 101.

[0046] Figure 3B illustrates an example GUI 310 generated by the account application 213. The GUI 310 may be associated with the GUI 300 of Figure 3A, e.g., the GUI 310 may be outputted subsequent to the GUI 300. As shown, the GUI 310 depicts an image 303 of a contactless card 101. The image 303 may be one of the card images 231 received from the DAM 225 based on the CMID of the contactless card 101 associated with the account of an authenticated user. The account application 213 may select the image 303 based on the card metadata 232 of the contactless card 101 and/or the device attributes 214 of the device 210. As shown, the image 303 of the contactless card 101 depicts the contactless card 101 in a vertical, face-up orientation, which may be determined to be the optimal orientation by the account application 213. As shown, the GUI 310 may further include a contact pad 304, which may be part of the optimal orientation determined by the account application 213. Doing so allows the user to subsequently tap the contactless card 101 to the device 210 according to the orientation and/or locations depicted in Figures 3A-3B.

[0047] Figure 4A illustrates an example GUI 400 generated by the account application 213 executing on a device 210. As shown, the GUI 400 includes an outline 401 (dashed lines) depicting where on the device 210 the user should place the contactless card 101 to enable data transfer (and/or enable faster data transfer relative to other orientations and/or placements). Furthermore, the GUI 400 includes an outline 402 of the contact pad of the contactless card 101. The GUI 400 may generally be based on the device attributes 214 of the device 210 and/or the card metadata 232 of the contactless card 101.

[0048] Figure 4B illustrates an example GUI 410 generated by the account application 213 executing on a device 210. The GUI 410 may be associated with the GUI 400 of Figure 4A, e.g., the GUI 410 may be outputted subsequent to the GUI 400. As shown, the GUI 410 includes an image 405 of a contactless card 101 according to a vertical, face-up orientation. The GUI 410 further includes a graphical contact pad 406, allowing the user to determine the proper orientation of the card 101 to the device 210. As shown, the image 405 of the contactless card 101 further includes one or more logos 407, 408 overlaid on the image 405. Furthermore, the image 405 includes overlaid user-specific attributes 409, e.g., card number, expiration date, CVV, and cardholder name.

[0049] Returning to Figure 4A, a front-facing camera 403 of the device 210 is depicted. The camera 403 may correspond to the camera 219 and may capture images used by the account application 213. For example, if the user places the contactless card 101 over the camera 403, an image captured by the camera 403 may be obscured by the card 101. Therefore, the account application 213 may determine whether data transfer has been initiated between the contactless card 101 and the device 210. If data transfer has not been initiated and the image captured by the camera 403 indicates the card is covering the camera 403, the account application 213 may output an alert to the user to adjust the orientation and/or location on the device 210 where the card is being tapped.

[0050] Figure 5A illustrates an example GUI 500 generated by the account application 213 executing on a device 210. The GUI 500 may generally be based on the device attributes 214 of the device 210 and/or the card metadata 232 of the contactless card 101. As shown, the GUI 500 includes an image 501 of a contactless card 101 and an image 502 of the device 210. The GUI 500 depicts the contactless card 101 being tapped to the rear surface of the mobile device 210.

[0051] Figure 5B illustrates an example GUI 510 generated by the account application 213. As shown, the GUI 510 depicts an image 503 of the contactless card 101 in a different position relative to the device 502. In some embodiments, the GUI 510 is generated responsive to the account application 213 determining data transfer has not been initiated between the card 101 and the device 210 within a threshold amount of time. As another example, the images 501, 503 may correspond to two default placement locations and/or orientations for the contactless card 101 relative to the device 210. Therefore, the account application 213 may output the GUI 500 and/or the GUI 510 to assist the user in ensuring that data transfer is initiated when tapping the contactless card 101 to a device 210.

[0052] Operations for the disclosed embodiments may be further described with reference to the following figures. Some of the figures may include a logic flow. Although such figures presented herein may include a particular logic flow, it can be appreciated that the logic flow

merely provides an example of how the general functionality as described herein can be implemented. Further, a given logic flow does not necessarily have to be executed in the order presented unless otherwise indicated. In addition, the given logic flow may be implemented by a hardware element, a software element executed by a processor, or any combination thereof. The embodiments are not limited in this context.

[0053] Figure 6 illustrates an embodiment of a logic flow 600. The logic flow 600 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 600 may include some or all of the operations to provide accurate images of contactless cards 101 in graphical user interfaces of the account application 213 to enable data transfer (e.g., between contactless cards 101 and devices 210). Embodiments are not limited in this context.

[0054] As shown, the logic flow 600 begins at block 610, where the account application 213 receives valid authentication credentials for an account. At block 620, the account application 213 may determine the device attributes 214 of a device 210 executing the account application 213. The account application 213 may further determine a CMID of a first contactless card 101 of one or more contactless cards 101 associated with the account. In embodiments where multiple cards 101 are associated with the account, the account application 213 may select the first card 101 based on the card that is being used as part of an operation in the account application 213 (e.g., balance transfer, virtual account number generation, etc.). At block 630, the account application 213 may receive one or more images 231 of the first contactless card 101 and one or more elements of card metadata 232 from the DAM system 225 based on the CMID of the first contactless card 101.

[0055] At block 640, the account application 213 may determine an optimal orientation and/or placement of the contactless card 101 to enable data transfer with the device 210. The optimal orientation and/or placement of the contactless card 101 may be based on the card metadata 232 and/or the device attributes 214. For example, the optimal orientation may be a face-up vertical orientation placed on the screen of the device 210. As another example, the optimal orientation may be a horizontal orientation with the card 101 face-down placed on the back side (e.g., the side without a display) of the device 210.

[0056] At block 650, the account application 213 may generate a GUI depicting a first image 231 of the contactless card 101 according to the determined optimal orientation and/or location. The GUI may further include instructions to tap the contactless card 101 to the device 210 according to the optimal orientation and/or placement. At block 660, the account application 213 may optionally overlay cardholder data on the image 231 of the contactless card 101. For example, the account application 213 may overlay the cardholder name, account number of the contactless card 101, CVV of the contactless card 101, and expiration date of the contactless card 101. At

block 670, the account application 213 may display the GUI on a display of the device 210. At block 680, NFC (or other wireless) data transfer may be performed between the contactless card 101 and the device 210.

[0057] Figure 7 illustrates an embodiment of a logic flow 700. The logic flow 700 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 700 may include some or all of the operations to provide accurate images of contactless cards 101 in graphical user interfaces of the account application 213. Embodiments are not limited in this context.

[0058] As shown, the logic flow 700 begins at block 710, where the camera 219 of a device 210 may capture an image depicting a contactless card 101. At block 720, the account application 213 may determine whether the correct contactless card 101 is being presented by the user. For example, if the user is attempting to generate a virtual account number for a first contactless card 101 may be required to tap the first contactless card 101 to the device 210. However, the account application 213 may analyze the image captured at block 710 to determine that a second contactless card 101, different than the first contactless card 101, is being held by the user. The account application 213 may determine that the first contactless card 101 is not being presented based on any suitable technique, such as whether the color, logos, and/or account numbers of the card depicted in the image match the corresponding color, logos, and/or account numbers of the first contactless card 101. Upon determining the user is not presenting the correct card, the account application 213 may output an indication at block 730 specifying that the incorrect contactless card 101 is being presented. The indication may be an audio indication (e.g., an error tone) and/or a visual indication (e.g., updating the GUI to inform the user that the incorrect card is detected).

[0059] At block 740, the account application 213 may instruct the camera 219 to capture a second image. The account application 213 may analyze the second image to determine that the second image depicts at least a portion of the contactless card 101 covering the camera 219. At block 750, the account application 213 may determine that data transfer between the device 210 and the contactless card 101 has not started (e.g., within a predefined time threshold). At block 760, the account application 213 may determine a different orientation and/or placement of the contactless card 101 relative to the device 210. At block 770, the account application 213 may output a GUI depicting the different orientation and/or placement of the contactless card 101 relative to the device 210.

[0060] Figure 8 illustrates an embodiment of an exemplary computing architecture 800 comprising a computing system 802 that may be suitable for implementing various embodiments as previously described. In various embodiments, the computing architecture 800 may comprise or be implemented as part of an electronic device. In some embodiments, the computing

architecture 800 may be representative, for example, of a system that implements one or more components of the system 100. In some embodiments, computing system 802 may be representative, for example, of the contactless card 101, mobile devices 210, and the server 220 of the system 200. The embodiments are not limited in this context. More generally, the computing architecture 800 is configured to implement all logic, applications, systems, methods, apparatuses, and functionality described herein with reference to Figures 1-7.

[0061] As used in this application, the terms “system” and “component” and “module” are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution, examples of which are provided by the exemplary computing architecture 800. For example, a component can be, but is not limited to being, a process running on a computer processor, a computer processor, a hard disk drive, multiple storage drives (of optical and/or magnetic storage medium), an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a server and the server can be a component. One or more components can reside within a process and/or thread of execution, and a component can be localized on one computer and/or distributed between two or more computers. Further, components may be communicatively coupled to each other by various types of communications media to coordinate operations. The coordination may involve the uni-directional or bi-directional exchange of information. For instance, the components may communicate information in the form of signals communicated over the communications media. The information can be implemented as signals allocated to various signal lines. In such allocations, each message is a signal. Further embodiments, however, may alternatively employ data messages. Such data messages may be sent across various connections. Exemplary connections include parallel interfaces, serial interfaces, and bus interfaces.

[0062] The computing system 802 includes various common computing elements, such as one or more processors, multi-core processors, co-processors, memory units, chipsets, controllers, peripherals, interfaces, oscillators, timing devices, video cards, audio cards, multimedia input/output (I/O) components, power supplies, and so forth. The embodiments, however, are not limited to implementation by the computing system 802.

[0063] As shown in Figure 8, the computing system 802 comprises a processor 804, a system memory 806 and a system bus 808. The processor 804 can be any of various commercially available computer processors, including without limitation an AMD® Athlon®, Duron® and Opteron® processors; ARM® application, embedded and secure processors; IBM® and Motorola® DragonBall® and PowerPC® processors; IBM and Sony® Cell processors; Intel® Celeron®, Core®, Core (2) Duo®, Itanium®, Pentium®, Xeon®, and XScale® processors; and

similar processors. Dual microprocessors, multi-core processors, and other multi-processor architectures may also be employed as the processor 804.

[0064] The system bus 808 provides an interface for system components including, but not limited to, the system memory 806 to the processor 804. The system bus 808 can be any of several types of bus structure that may further interconnect to a memory bus (with or without a memory controller), a peripheral bus, and a local bus using any of a variety of commercially available bus architectures. Interface adapters may connect to the system bus 808 via a slot architecture. Example slot architectures may include without limitation Accelerated Graphics Port (AGP), Card Bus, (Extended) Industry Standard Architecture ((E)ISA), Micro Channel Architecture (MCA), NuBus, Peripheral Component Interconnect (Extended) (PCI(X)), PCI Express, Personal Computer Memory Card International Association (PCMCIA), and the like.

[0065] The system memory 806 may include various types of computer-readable storage media in the form of one or more higher speed memory units, such as read-only memory (ROM), random-access memory (RAM), dynamic RAM (DRAM), Double-Data-Rate DRAM (DDRAM), synchronous DRAM (SDRAM), static RAM (SRAM), programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), flash memory (e.g., one or more flash arrays), polymer memory such as ferroelectric polymer memory, ovonic memory, phase change or ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, magnetic or optical cards, an array of devices such as Redundant Array of Independent Disks (RAID) drives, solid state memory devices (e.g., USB memory, solid state drives (SSD) and any other type of storage media suitable for storing information. In the illustrated embodiment shown in Figure 8, the system memory 806 can include non-volatile memory 810 and/or volatile memory 812. A basic input/output system (BIOS) can be stored in the non-volatile memory 810.

[0066] The computing system 802 may include various types of computer-readable storage media in the form of one or more lower speed memory units, including an internal (or external) hard disk drive (HDD) 814, a magnetic floppy disk drive (FDD) 816 to read from or write to a removable magnetic disk 818, and an optical disk drive 820 to read from or write to a removable optical disk 822 (e.g., a CD-ROM or DVD). The HDD 814, FDD 816 and optical disk drive 820 can be connected to the system bus 808 by a HDD interface 824, an FDD interface 826 and an optical drive interface 828, respectively. The HDD interface 824 for external drive implementations can include at least one or both of Universal Serial Bus (USB) and IEEE 1394 interface technologies. The computing system 802 is generally is configured to implement all logic, systems, methods, apparatuses, and functionality described herein with reference to Figures 1-7.

[0067] The drives and associated computer-readable media provide volatile and/or nonvolatile storage of data, data structures, computer-readable instructions, computer-executable instructions, and so forth. For example, a number of program modules can be stored in the drives and memory units 810, 812, including an operating system 830, one or more application programs 832, other program modules 834, and program data 836. In one embodiment, the one or more application programs 832, other program modules 834, and program data 836 can include, for example, the various applications and/or components of the systems 100 and/or 200, e.g., the applet 103, private key 104, encrypted data 105, customer ID 107, CMID 108, account application 213, the authentication application 223, account data 224, and DAM system 225.

[0068] A user can enter commands and information into the computing system 802 through one or more wire/wireless input devices, for example, a keyboard 838 and a pointing device, such as a mouse 840. Other input devices may include microphones, infra-red (IR) remote controls, radio-frequency (RF) remote controls, game pads, stylus pens, card readers, dongles, finger print readers, gloves, graphics tablets, joysticks, keyboards, retina readers, touch screens (e.g., capacitive, resistive, etc.), trackballs, trackpads, sensors, styluses, and the like. These and other input devices are often connected to the processor 804 through an input device interface 842 that is coupled to the system bus 808, but can be connected by other interfaces such as a parallel port, IEEE 1394 serial port, a game port, a USB port, an IR interface, and so forth.

[0069] A monitor 844 or other type of display device is also connected to the system bus 808 via an interface, such as a video adaptor 846. The monitor 844 may be internal or external to the computing system 802. In addition to the monitor 844, a computer typically includes other peripheral output devices, such as speakers, printers, and so forth.

[0070] The computing system 802 may operate in a networked environment using logical connections via wire and/or wireless communications to one or more remote computers, such as a remote computer 848. The remote computer 848 can be a workstation, a server computer, a router, a personal computer, portable computer, microprocessor-based entertainment appliance, a peer device or other common network node, and typically includes many or all of the elements described relative to the computing system 802, although, for purposes of brevity, only a memory/storage device 850 is illustrated. The logical connections depicted include wire/wireless connectivity to a local area network (LAN) 852 and/or larger networks, for example, a wide area network (WAN) 854. Such LAN and WAN networking environments are commonplace in offices and companies, and facilitate enterprise-wide computer networks, such as intranets, all of which may connect to a global communications network, for example, the Internet. In embodiments, the network 230 of Figure 2 is one or more of the LAN 852 and the WAN 854.

[0071] When used in a LAN networking environment, the computing system 802 is connected to the LAN 852 through a wire and/or wireless communication network interface or adaptor 856. The adaptor 856 can facilitate wire and/or wireless communications to the LAN 852, which may also include a wireless access point disposed thereon for communicating with the wireless functionality of the adaptor 856.

[0072] When used in a WAN networking environment, the computing system 802 can include a modem 858, or is connected to a communications server on the WAN 854, or has other means for establishing communications over the WAN 854, such as by way of the Internet. The modem 858, which can be internal or external and a wire and/or wireless device, connects to the system bus 808 via the input device interface 842. In a networked environment, program modules depicted relative to the computing system 802, or portions thereof, can be stored in the remote memory/storage device 850. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers can be used.

[0073] The computing system 802 is operable to communicate with wired and wireless devices or entities using the IEEE 802 family of standards, such as wireless devices operatively disposed in wireless communication (e.g., IEEE 802.16 over-the-air modulation techniques). This includes at least Wi-Fi (or Wireless Fidelity), WiMax, and Bluetooth™ wireless technologies, among others. Thus, the communication can be a predefined structure as with a conventional network or simply an ad hoc communication between at least two devices. Wi-Fi networks use radio technologies called IEEE 802.11x (a, b, g, n, etc.) to provide secure, reliable, fast wireless connectivity. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wire networks (which use IEEE 802.3-related media and functions).

[0074] Various embodiments may be implemented using hardware elements, software elements, or a combination of both. Examples of hardware elements may include processors, microprocessors, circuits, circuit elements (e.g., transistors, resistors, capacitors, inductors, and so forth), integrated circuits, application specific integrated circuits (ASIC), programmable logic devices (PLD), digital signal processors (DSP), field programmable gate array (FPGA), logic gates, registers, semiconductor device, chips, microchips, chip sets, and so forth. Examples of software may include software components, programs, applications, computer programs, application programs, system programs, machine programs, operating system software, middleware, firmware, software modules, routines, subroutines, functions, methods, procedures, software interfaces, application program interfaces (API), instruction sets, computing code, computer code, code segments, computer code segments, words, values, symbols, or any combination thereof. Determining whether an embodiment is implemented using hardware

elements and/or software elements may vary in accordance with any number of factors, such as desired computational rate, power levels, heat tolerances, processing cycle budget, input data rates, output data rates, memory resources, data bus speeds and other design or performance constraints.

[0075] One or more aspects of at least one embodiment may be implemented by representative instructions stored on a machine-readable medium which represents various logic within the processor, which when read by a machine causes the machine to fabricate logic to perform the techniques described herein. Such representations, known as “IP cores” may be stored on a tangible, machine readable medium and supplied to various customers or manufacturing facilities to load into the fabrication machines that make the logic or processor. Some embodiments may be implemented, for example, using a machine-readable medium or article which may store an instruction or a set of instructions that, if executed by a machine, may cause the machine to perform a method and/or operations in accordance with the embodiments. Such a machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware and/or software. The machine-readable medium or article may include, for example, any suitable type of memory unit, memory device, memory article, memory medium, storage device, storage article, storage medium and/or storage unit, for example, memory, removable or non-removable media, erasable or non-erasable media, writeable or re-writeable media, digital or analog media, hard disk, floppy disk, Compact Disk Read Only Memory (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewritable (CD-RW), optical disk, magnetic media, magneto-optical media, removable memory cards or disks, various types of Digital Versatile Disk (DVD), a tape, a cassette, or the like. The instructions may include any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, encrypted code, and the like, implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language.

[0076] The foregoing description of example embodiments has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed. Many modifications and variations are possible in light of this disclosure. It is intended that the scope of the present disclosure be limited not by this detailed description, but rather by the claims appended hereto. Future filed applications claiming priority to this application may claim the disclosed subject matter in a different manner, and may generally include any set of one or more limitations as variously disclosed or otherwise demonstrated herein.