

Technical Disclosure Commons

Defensive Publications Series

May 2023

GENERIC TRANSACTION CARD

PALAKH SHANGLE
VISA

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

SHANGLE, PALAKH, "GENERIC TRANSACTION CARD", Technical Disclosure Commons, (May 29, 2023)
https://www.tdcommons.org/dpubs_series/5928



This work is licensed under a [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/).

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

“GENERIC TRANSACTION CARD”

VISA

INVENTOR:

PALAKH SHANGLE

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to a generic transaction card, and particularly to a generic transaction card authorization method for approving a child lock credit card.

BACKGROUND

[0002] In general, credit cards and/or debit cards are widely used around the world as a form of financial transaction for goods/services. Several credit cards may be issued for one credit card account, and all transactions made with any of the cards are treated identically. One of the main challenges associated with giving children credit card access is ensuring that they use them responsibly and do not incur large debts. Parents who cannot consistently monitor their child's spending habits may find it more difficult. For example, expenditures may vary widely from the cost of lunch to the cost of a new online game and parents may be unable to monitor expenditures made by a child. Therefore, parental control of a child's credit card expenditures is limited by the current system.

[0003] Another challenge is the risk of fraud and identity theft, for example, if the child loses the credit card or if it is stolen. This can result in unauthorized charges that the parent may not be able to recover. In other words, parents may simply need to pay for a child's expenditure. In traditional payment instruments, bank-issued card information may be easily copied and card passwords may be easily cracked which leads to safety issues. Therefore, there is a need for a child lock credit card and method enabling the child lock credit card that addresses the disadvantages described above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0005] **FIG. 1** illustrates an exemplary flow of a method for issuing a generic transaction card, in accordance with some embodiments of the present disclosure;

[0006] **FIG. 2** discloses an exemplary embodiment of the method and a transaction authentication process flow using the generic transaction card, in accordance with some embodiments of the present disclosure; and

[0007] **FIG. 3** is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0008] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

[0009] It is to be understood that the present disclosure may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings and described in the following specification are simply exemplary and non-limiting embodiments or aspects. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0010] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0011] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0012] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus preceded by “comprises... a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0013] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0014] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to" unless expressly specified otherwise.

[0015] As used herein, the terms “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to receive information directly or indirectly from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit (e.g., a third unit located between the first unit and the second unit) processes information received from the first unit and communicates the processed information to the second unit. In some non-limiting embodiments, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0016] As used herein, the term “computing device” may refer to one or more electronic devices that are configured to communicate with directly or indirectly or over one or more networks. A computing device may be a mobile or portable computing device, a desktop computer, a server, and/or the like. Furthermore, the term “computer” may refer to any computing device that includes the necessary components to receive, process, and output data, and normally includes a display, a processor, a memory, an input device, and a network interface. A “computing system” may include one or more computing devices or computers.

[0017] As used herein, the term “application” or “Application Program Interface” (API) may refer to computer code or other data stored on a computer-readable medium that may be executed by a processor to facilitate the interaction between software components, such as a client-side front-end and/or server-side back-end for receiving data from the client. An “interface” refers to a generated display, such as one or more graphical user interfaces (GUIs) with which a user may interact, either directly or indirectly (e.g., through a keyboard, mouse, touchscreen, etc.). Further, multiple computers, e.g., servers, or other computerized devices, such as an autonomous vehicle including a vehicle computing system, directly or indirectly communicating in the network environment may constitute a “system” or a “computing system”.

[0018] As used herein, the term "mobile device" may refer to any electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (e.g., cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, wearable devices (e.g., watches), vehicles (e.g., cars), etc. A mobile device may comprise any suitable hardware and software for performing such functions and may also include multiple devices or components (e.g., when a device has remote access to a network by tethering to another device - i.e., using the other device as a relay - both devices taken together may be considered a single mobile device).

[0019] As used herein, the term "Authentication data" may refer to any data suitable for authenticating a user or mobile device. Authentication data may be obtained from a user or a

device that is operated by the user. Examples of authentication data obtained from a user may include PINs (personal identification numbers), passwords, etc. Examples of authentication data that may be obtained from a device may include device serial numbers, hardware secure element identifiers, device fingerprints, phone numbers, IMEI numbers, etc.

[0020] **FIG. 1** illustrates an exemplary flow of a method for issuing a generic transaction card, in accordance with some embodiments of the present disclosure.

[0021] As illustrated, the method for issuing a generic transaction card is implemented via an environment 100. The environment 100 comprises a first user device 101, a parental control system 103, a bank server 105, and a child lock credit card 107 (hereinafter referred to as card 107). The first user device 101 may be associated with a first user, also be referred to as a parent or head of the family member, or account holder. The bank server 105 is associated with issuer bank which is the customer bank that issues the credit or debit card on behalf of the card schemes. In an embodiment, the first user, via the first user device 101, requests for issuance of the card 107 by applying to the bank server 105. The card 107 may be a physical credit or debit card associated with parents or first user's account number. In one embodiment, the card 107 may be a child lock credit card or a child lock debit card issued to individuals or parents by the issuing bank server 105. The card 107 may also have a credit limit which is set by the first user of the first user device 101. The parental control system 103 is configured to establish and enforce the restrictions on the card 107, wherein the restrictions are set by the first user via the first user device 101. The first user may send a request to the parental control system 103 via the first user device 101 through a web portal or mobile Application (App) for configuring restrictions on the card 107. In one embodiment, the first user may configure restrictions on the card 107 such as setting spending limits, types of purchases that are allowed through the card 107 and so on. The first user may also view transaction history of all transactions made on the card 107 stored on a memory storage associated with the parental control system 103. The parental control system 103 comprises records of child lock credit card transactions, including, debits, credits, payments and other transaction details. Upon determining completion of configuration of the restrictions on the card 107, the parental control system 103 transmits a signal indicating the same to the bank server 105. Thereafter, the bank server 105 processes the application submitted by the first user device 101 and issues the card 107, for example, the child lock credit card to the first user to withdraw cash or purchase goods online.

[0022] **FIG. 2** discloses an exemplary embodiment of the method and the transaction authentication process flow using the generic transaction card, in accordance with some embodiments of the present disclosure.

[0023] As illustrated, the exemplary environment 200 of a generic transaction card authentication process includes a second user 201, a merchant payment system 203 associated with a merchant, a card authorization system 207 and a data storage 209 connected via a network 210. The second user 201 may also be a child in the family, or any family member associated with the first user. The merchant payment system 203 may be an individual or entity selling goods and/or services, or providing access to goods and/or services, to users (for example, users or customers) based on a transaction, say a financial transaction. The merchant payment system 203, the card authorization system 207 and the data storage 209 may be interconnected (for example, establish a connection to communicate) via wired connections, wireless connections, or a combination of wired and wireless connections. The card authorization system 207 may include one or more devices capable of sending or receiving information and/or data to/from the merchant payment system 203, via the network 210.

[0024] The network 210 may include one or more wired and/or wireless network. For example, the network 210 may include a cellular network (e.g., a long-term evolution (LTE) network, a third generation (3G) network, a fourth generation (4G) network, a code division multiple access (CDMA) network, etc.), a public land mobile network (PLMN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), a telephone network (e.g., the public switched telephone network (PSTN)), a private network, an ad hoc network, an intranet, the Internet, a fiber optic-based network, a cloud computing network, and/or the like, and/or a combination of these or other types of networks.

[0025] In an embodiment, a child wishes to make an expenditure or make a purchase of any goods by using a child lock credit card. In particular, the second user 201 may use the card 107 to make purchases or conduct transactions by presenting the card 107 to the merchant payment system 203. Thereafter, the merchant payment system 203 sends a request for authorization to the card authorization system 207 via the network 210 to verify one or more conditions in the transaction. The one or more conditions include without limiting to, credit card funds status to complete a financial transaction and the compliance of the transaction with any restrictions set by the first user device 101. The card authorization system 207 communicates with the bank

server 105 to verify the compliance of the transaction with the restrictions set by the first user and request for the credit if the verification of compliance is successful. The bank server 105 issues the credit to the card authorization system 207 and approves the transaction to the card authorization system 207. Thereafter, the card authorization system 207 sends an approval message back to the merchant payment system 203 and indicates the completion of the financial transaction. In another embodiment, if the card authorization system 207 receives a rejection message from the bank server 105 upon unsuccessful compliance of the restrictions, the card authorization system 207 declines the transaction to the merchant payment system 203, hence blocking unauthorized or restricted transactions set by the first user. Further, the card authorization system 207 stores the transaction information in the transaction data storage 209 for further usage. The data storage 209 may store information and/or software related to the operation of the card authorization system 207. For example, data storage 209 may include a hard disk (for example, a magnetic disk, an optical disk, a magneto-optic disk, a solid-state disk, and so on), a compact disc (CD), a digital versatile disc (DVD), a floppy disk, a cartridge, a magnetic tape, and/or another type of computer-readable medium, along with a corresponding drive. The transaction information may include the data, time, amount spent by the second user 201, merchant details and spending activity. As a result, the present disclosure ensures that transactions made with a child lock credit card are secure, controlled, and in compliance with the restrictions set by the parent.

Advantages of the present invention:

[0026] In an embodiment, the present disclosure discloses a generic transaction card authorization method for approving a second user credit card transaction.

[0027] In an embodiment, the present disclosure provides a secure and controlled environment for second user, for example, children to use credit cards. For example, if the card is lost or stolen, the present disclosure helps in blocking any new authorizations on the card and protects from fraud.

[0028] In an embodiment, the present disclosure helps parents to set restrictions on spending funds.

[0029] In an embodiment, the present disclosure allows a parent to provide a supervised credit card to a child.

[0030] In an embodiment, the present disclosure enables parents to restrict certain types of purchases made by their child and keep track of their children's spending activity including spending statements.

General computer system:

[0031] FIG. 3 illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0032] In an embodiment, FIG. 3 illustrates a block diagram of an exemplary computer system 300 which may be used to implement the system in accordance with the present disclosure. The computer system 300 may include a central processing unit ("CPU" or "processor") 302. In some embodiments, the computer system 300 may be a card authorization system 207 to perform authentication of the second user 201 credit card transaction via a network interface 303 and communication network 309. The processor 302 may include at least one data processor for authorizing the second user 201 credit card transaction based on the inputs received from a merchant payment system 203 and a data storage 209 to store approved transaction information via a network interface 303 and communication network 309. The processor 302 may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0033] The processor 302 may be disposed in communication with one or more Input/Output (I/O) devices (312 and 313) via I/O interface 301. The I/O interface 301 employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, Radio Corporation of America (RCA) connector, stereo, IEEE-1394 high speed serial bus, serial bus, Universal Serial Bus (USB), infrared, Personal System/2 (PS/2) port, Bbayonet Neill-Concelman (BNC) connector, coaxial, component, composite, Digital Visual Interface (DVI), High-Definition Multimedia Interface (HDMI), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (VGA), IEEE 802.11b/g/n/x, Bluetooth, cellular e.g., Code-Division Multiple Access (CDMA), High-Speed Packet Access (HSPA+), Global System for Mobile communications (GSM), Long-Term Evolution (LTE), Worldwide Interoperability for Microwave access (WiMax), or the like, etc.

[0034] Using the I/O interface 301, the computer system 300 may communicate with one or more I/O devices such as input devices 312 and output devices 313. For example, the input devices 312 may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output devices 313 may be a printer, fax machine, video display (e.g., Cathode Ray Tube (CRT), Liquid Crystal Display (LCD), Light-Emitting Diode (LED), plasma, Plasma Display Panel (PDP), Organic Light-Emitting Diode display (OLED) or the like), audio speaker, etc.

[0035] In some embodiments, the processor 302 may be disposed in communication with a communication network 309 via a network interface 303. The network interface 303 may communicate with the communication network 309. The network interface 303 may employ connection protocols including, without limitation, direct connect, ethernet (e.g., twisted pair 10/100/1000 Base T), Transmission Control Protocol/Internet Protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network 309 may include, without limitation, a direct interconnection, Local Area Network (LAN), Wide Area Network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. Using the network interface 303 and the communication network 309, the computer system 300 may communicate with a database 314, which may be the enrolled templates database 313. The network interface 303 may employ connection protocols include, but not limited to, direct connect, ethernet (e.g., twisted pair 10/100/1000 Base T), Transmission Control Protocol/Internet Protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc.

[0036] The communication network 309 includes, but is not limited to, a direct interconnection, a Peer-to-Peer (P2P) network, Local Area Network (LAN), Wide Area Network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi and such. The communication network 309 may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the communication network 309 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0037] In some embodiments, the processor 302 may be disposed in communication with a memory 305 (e.g., RAM, ROM, etc. not shown in Fig. 3) via a storage interface 304. The

storage interface 304 may connect to memory 305 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as, Serial Advanced Technology Attachment (SATA), Integrated Drive Electronics (IDE), IEEE-1394, Universal Serial Bus (USB), fiber channel, Small Computer Systems Interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

[0038] The memory 305 may store a collection of program or database components, including, without limitation, user interface 306, an operating system 307, a web browser 308 etc. In some embodiments, computer system 300 may store user/application data, such as, the data, variables, records, etc., as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle or Sybase.

[0039] The operating system 307 may facilitate resource management and operation of the computer system 300. Examples of operating systems include, without limitation, AppleTM MacintoshTM OS XTM, UNIXTM, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSDTM, Net BSDTM, Open BSDTM, etc.), Linux distributions (e.g., Red HatTM, UbuntuTM, K-UbuntuTM, etc.), International Business Machines (IBMTM) OS/2TM, Microsoft WindowsTM (XPTM, Vista/7/8, etc.), Apple iOSTM, Google AndroidTM, BlackberryTM operating system (OS), or the like. The User interface 306 may facilitate display, execution, interaction, manipulation, or operation of program components through textual or graphical facilities. For example, user interfaces may provide computer interaction interface elements on a display system operatively connected to the computer system 300, such as cursors, icons, checkboxes, menus, scrollers, windows, widgets, etc. Graphical User Interfaces (GUIs) may be employed, including, without limitation, Apple[®] Macintosh[®] operating systems' Aqua[®], IBM[®] OS/2[®], Microsoft[®] Windows[®] (e.g., Aero, Metro, etc.), web interface libraries (e.g., ActiveX[®], Java[®], Javascript[®], AJAX, HTML, Adobe[®] Flash[®], etc.), or the like.

[0040] In some embodiments, the computer system 300 may implement web browser 308 stored program components. Web browser 308 may be a hypertext viewing application, such as MicrosoftTM Internet ExplorerTM, Google ChromeTM, Mozilla FirefoxTM, AppleTM SafariTM, etc. Secure web browsing may be provided using secure hypertext transport protocol (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc. Web browsers 308 may utilize facilities such as AJAX, DHTML, AdobeTM Flash, Javascript, Application

Programming Interfaces (APIs), etc. In some embodiments, the computer system 300 may implement a mail server stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as ASP, ActiveX, ANSI C++/C#, Microsoft .NET, Common Gateway Interface (CGI) scripts, Java, JavaScript, PERL, PHP, Python, WebObjects, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), Microsoft Exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like.

[0041] In some embodiments, the computer system 300 may implement a mail client stored program component. The mail client may be a mail viewing application, such as APPLE[®] MAIL, MICROSOFT[®] ENTOURAGE[®], MICROSOFT[®] OUTLOOK[®], MOZILLA[®] THUNDERBIRD[®], etc.

[0042] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer-readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0043] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer-readable medium”, where a processor may read and execute the code from the computer-readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries. A non-transitory computer-readable medium may include media such as magnetic storage medium (e.g., hard disk drives, floppy disks, tape, etc.), optical storage (CD-ROMs, DVDs, optical disks, etc.), volatile and non-volatile memory devices (e.g., EEPROMs, ROMs,

PROMs, RAMs, DRAMs, SRAMs, Flash Memory, firmware, programmable logic, etc.), etc. Further, non-transitory computer-readable media may include all computer-readable media except for a transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0044] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items or meant to be limited to only the listed item or items. It must also be noted that as used herein, the singular forms "a," "an," and "the" include plural references unless the context clearly dictates otherwise.

[0045] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term "computer-readable medium" should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0046] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or

circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0047] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

“GENERIC TRANSACTION CARD”

ABSTRACT

The present disclosure relates to a generic transaction card authorization method for approving a second user credit card transaction. The present disclosure suggests receiving a request from a first user via a first user device to a bank server for issuing a credit card through a parental control system, wherein the parental control system is used for setting and enforcing the restrictions on the credit card. The bank server processes the request and issues the card to the first user. Thereafter, the present disclosure suggests using, by a second user, the issued credit card for financial transactions at a merchant payment system. The merchant payment system consequently submits a request to a card authorization system to verify financial transactions via a network. Further, the present disclosure suggests sending an approval message to the merchant payment system after verification to complete the financial transaction.

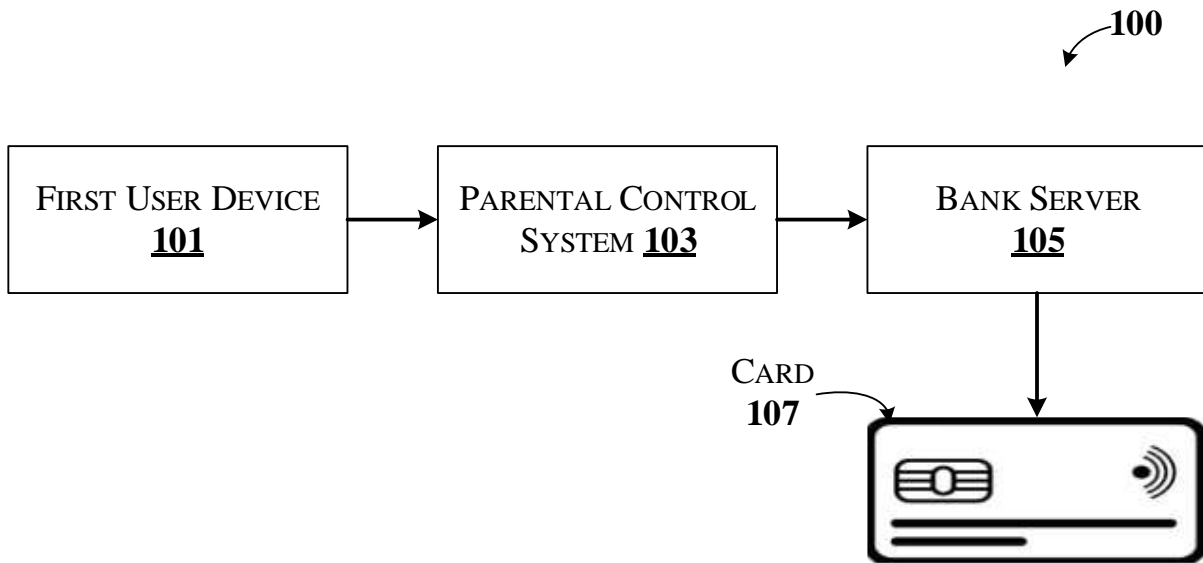


FIG. 1

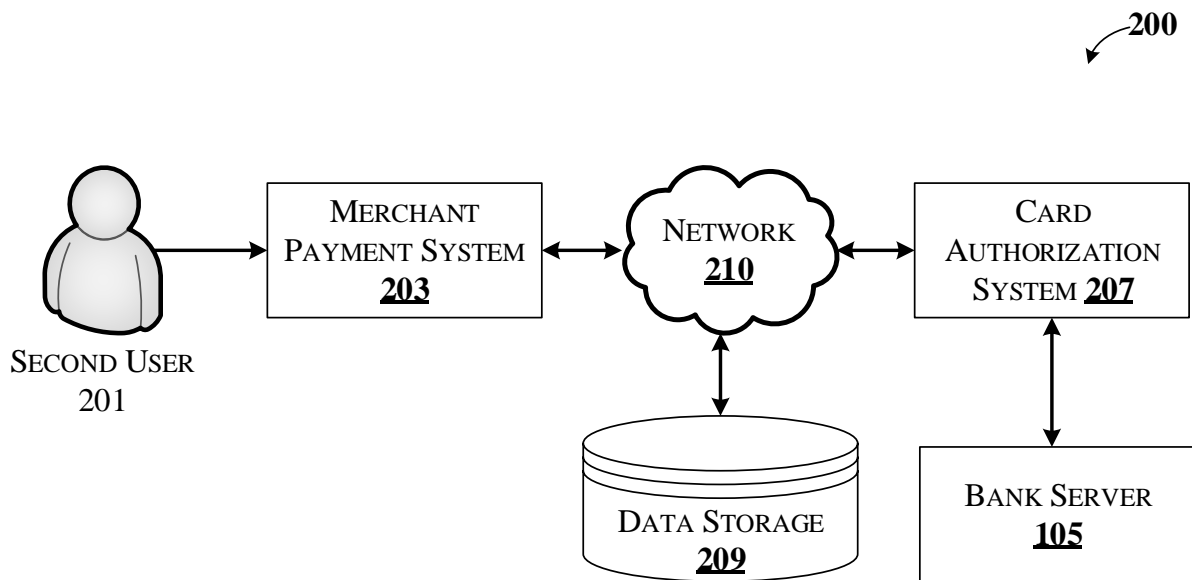


FIG. 2

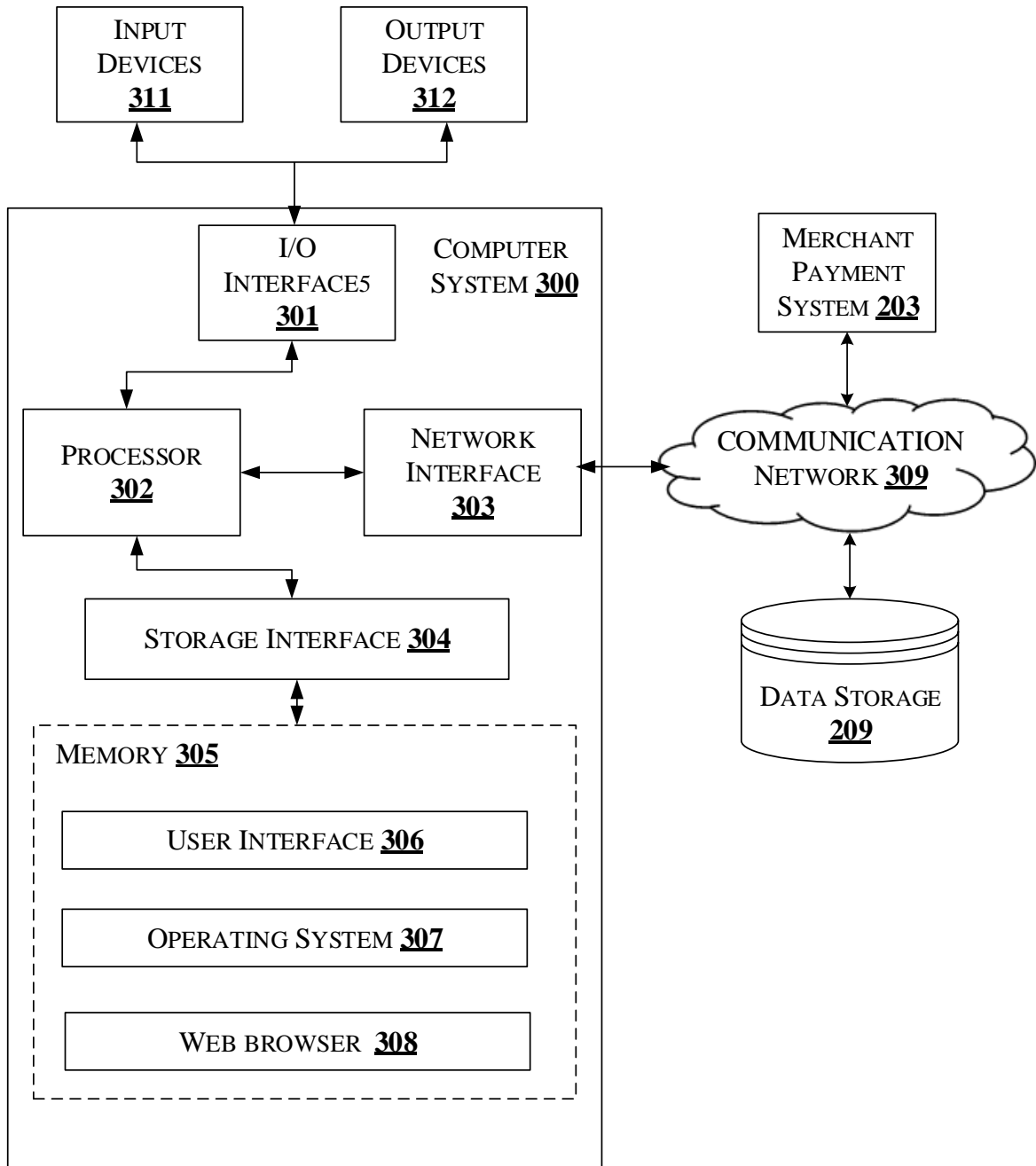


FIG. 3