

A NETWORK-ENABLED SMART APPARATUS AND SYSTEMS AND METHODS FOR ACTIVATING AND PROVISIONING SAME

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Patent Application No. 17/213,943 filed March 26, 2021, the disclosure of which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

[0002] This disclosure relates generally to network-enabled appliances and other apparatus, and, more particularly, to systems and methods for activating network-enabled apparatus using web-based near field communication (NFC) protocols.

BACKGROUND OF THE INVENTION

[0003] Many home appliances, vehicles, and IT systems now have virtually immediate network connectivity upon installation in the home. Typical activation procedures, however, require the homeowner to connect the new appliance or other apparatus to their home network, then download an installation application to their home computer or mobile device. The application then walks the homeowner through the process of activating and provisioning the new apparatus according to the homeowner's use preferences. Typically, this requires the user to locate and enter identification information for the new device. The application may also require that the homeowner provide account information required for management or use of the device.

SUMMARY OF THE INVENTION

[0004] An illustrative aspect of the invention provides network-enabled apparatus comprising an apparatus data processing system, at least one operational system in communication with the apparatus data processing system and configured for carrying out a mechanical or electrical operation, a first network communication interface configured for establishing communication over a wide area network, a second network communication interface configured for establishing

communication over a local network, and a memory. The memory has stored therein apparatus identification information, at least one service application comprising instructions for the apparatus data processing system to implement a service operation using the at least one operational system, and an activation application. The activation application comprises instructions for the apparatus data processing system to establish an internet connection via the first network communication interface and create an NFC-enabled web page. The application further comprises instructions to transmit, to a user device via the second communication interface, an instruction to navigate to the NFC-enabled web page and instructions to transmit to the user device via the NFC-enabled web page an instruction for a user of the user device to tap an NFC-enabled smart transaction card to the user device. The activation application also comprises instructions to read, via the NFC-enabled web page, NFC information transmitted to the user device by the smart transaction card. The NFC information includes card identification information unique to the smart transaction card. The activation application still further comprises instructions to transmit the NFC information and the apparatus identification information to a service administration server, and receive, from the service administration server, a service activation command. Responsive to the service activation command, the application will cause activation of at least one of the at least one service application.

[0005] Another aspect of the invention provides a method for activating a network-enabled apparatus using an NFC-enabled user device and an NFC-enabled smart transaction card associated with a card account. The method comprises establishing an internet connection by the network-enabled apparatus, creating an NFC-enabled web page by the network-enabled apparatus, and transmitting, by the network-enabled apparatus to the user device, an instruction to navigate to the NFC-enabled web page. The method further comprises transmitting, by the

network-enabled apparatus to the user device via the NFC-enabled web page, an instruction for the user to tap the smart transaction card to the user device, and reading, by the network-enabled apparatus via the NFC-enabled web page, NFC information transmitted to the user device by the smart transaction card. The NFC information includes card identification information unique to the smart transaction card. The method still further comprises transmitting, by the network-enabled apparatus to a service administration server of a service administrator, the NFC information and apparatus identification information, identifying, by the service administration server using the apparatus identification information, the network-enabled apparatus, and transmitting the NFC information by the service administration server to a card administration server. The method also comprises receiving, by the service administration server from the card administration server, card account information associated with the card account, identifying an account holder by the service administration server using the card account information, and associating, by the service administration server, the network-enabled apparatus with the card account and an apparatus service account with the service administrator. The method further comprises transmitting, by the service administration server to the network-enabled apparatus, a service activation command.

[0006] Another aspect of the invention provides a method for activating a network-enabled apparatus using an NFC-enabled user device and an NFC-enabled smart transaction card associated with a card account. The method comprises establishing communication between the network-enabled apparatus and the user device, creating an NFC-enabled web page by the network-enabled apparatus, and navigating to the NFC-enabled webpage by a web browser on the user device. The method further comprises establishing NFC communication between the smart transaction card and the user device and reading, by the network-enabled apparatus via the

NFC-enabled web page, NFC information transmitted to the user device by the smart transaction card. The NFC information includes card identification information unique to the smart transaction card. The method still further comprises transmitting, by the network-enabled apparatus to a service administration server, the NFC information and apparatus identification information and transmitting the NFC information by the service administration server to a card administration server. The method also comprises identifying, by the card administration server using the NFC information, a card account associated with the smart transaction card and transmitting, by the card administration server to the service administration server, card account information associated with the card account. The method yet further comprises identifying an account holder by the service administration server using the card account information, associating, by the service administration server, the network-enabled apparatus with the card account and an apparatus service account with the service administrator, and transmitting, by the service administration server to the network-enabled apparatus from the service administration server, a service activation command.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The invention can be more fully understood by reading the following detailed description together with the accompanying drawings, in which like reference indicators are used to designate like elements, and in which:

[0008] Figure 1 is a sequence diagram illustrating an operational scenario of an embodiment of the invention;

[0009] Figure 2 is a schematic representation of a home network having network-enabled smart apparatus usable in conjunction with methods of the invention;

[0010] Figure 3 is a schematic representation of a smart apparatus usable in embodiments of the

invention;

[0011] Figure 4 is a schematic representation of a user processing device usable in conjunction with methods of the invention;

[0012] Figure 5 is a schematic representation of a network-based system for activating a network-enabled smart apparatus according to an embodiment of the invention;

[0013] Figure 6 is a schematic representation of a microprocessor chip of a transaction card usable in embodiments of the invention;

[0014] Figure 7 is a schematic representation of an apparatus service administration server usable in embodiments of the invention;

[0015] Figure 8 is a schematic representation of card account administration server usable in embodiments of the invention;

[0016] Figure 9 is a flow chart of a method of activating a smart apparatus according to an embodiment of the invention;

[0017] Figure 10 is a flow chart of a method of activating a smart apparatus according to an embodiment of the invention; and

[0018] Figure 11 is a flow chart of a method of activating a smart apparatus according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0019] While the invention will be described in connection with particular embodiments and manufacturing environments, it will be understood that the invention is not limited to these embodiments and environments. On the contrary, it is contemplated that various alternatives, modifications and equivalents are included within the spirit and scope of the invention as described.

[0020] The present invention provides systems and methods for activating and provisioning various network-connected smart appliances and other apparatus. As homes become integrated via the “Internet of things”, homeowners are finding that every time they purchase a new appliance, they must go through an elaborate process to add the appliance to their home network, establish service, and configure the appliance to fit their needs. This process may be required for any uniquely identifiable smart appliance or device (i.e. any device having a network-enabled processing system). In a typical prior art scenario, a user purchases a device such as a Wi-Fi router for use in conjunction with an Internet service provider (ISP). The user must establish an account with the ISP and then may be asked to download an application for use in initializing the router and establishing Internet service. The app may require the user to log on to the user’s account, then scan a barcode on the bottom of the router. The ISP then associates the router with the user account and steps the user through a series of queries that can be used to establish service and configure the router.

[0021] In the methods of the present invention, the appliance or other apparatus may be provided with the capability of establishing its own web page which can be used to obtain information from an NFC-capable transaction card via the user’s mobile or other device. This can be accomplished without the need for an application on the mobile device with API calls configured for reading and interpreting the NFC information from the transaction card. The transaction card information may be read directly by the smart device and then passed to the ISP or other service provider, which may use the card information to identify the user and establish service. This provides for enhanced efficiency and security of the service initialization process as well as simplifying the process for the user.

[0022] NFC works using magnetic induction. The powered NFC reader creates a magnetic field

in which a transmitter (typically unpowered) may be immersed. Immersion in the magnetic field produces a current within the transmitter that can be used to power transmission of data to the receiver. NFC capability may be incorporated into transaction processing devices (e.g., merchant check-out devices) or into mobile and other user devices. The NFC transmitter may be a passive tag or, as will be discussed in more detail below, may be incorporated into a smart transaction card.

[0023] While NFC capability may be built into a user device, the ability to interpret NFC-transmitted information from a tag or other transmitter requires the use of an application on-board the user device. For example, if a mobile device is to read and interpret a tag's unique identifier, the user must open the application before establishing NFC communication with the tag. The tag may then be brought into NFC range of the user device, whereupon the device reads and interprets the tag's identifier. Absent the application, the NFC information can be "read" but the information is unusable.

[0024] To avoid the need for an NFC application to be loaded on the user device, embodiments of the invention make use of browser-based NFC (referred to herein as "Web NFC"). Web NFC is a simplified API for using NFC via web page JavaScript. Web NFC uses a high level approach instead of a powerful low level API that requires special privileges. In short, Web NFC allows the reading of NFC tags through a browser on the user device. This means that no additional application needs to be downloaded to the user device. The NFC-transmitted information is simply passed through the user device to the server or apparatus operating through the web page.

[0025] As will be discussed in more detail below, the methods of the invention may be used in conjunction with a typical home network and appliance control system having one or more

network-enabled smart apparatus connected to a user device via a local network. (See Figure 2.)

The user device and the smart apparatus may also be connected to a wide area network that allows communication between these devices and an ISP and/or one or more other service providers associated with the operation of the smart apparatus. (See Figure 5.)

[0026] An exemplary scenario for a method of the invention may follow a sequence of operations for initializing and provisioning a network-enabled smart apparatus as shown in Figure 1. In this scenario, a user purchases or otherwise obtains a network-enabled smart apparatus, powers it up and connects it to the Internet. The Internet connection may be, for example, via wired or wireless connection to a modem or Wi-Fi server. The smart apparatus then uses the Internet connection to create a web page. In some embodiments, the smart apparatus may instead contact a service administration server and request that a web page be created. Once the web page has been established, the smart apparatus communicates the web page address to the user device at 1100. Communication with the user device may be established by connecting the apparatus to the home network. In some embodiments, however, the apparatus may be configured to operate as a limited range wireless access point (i.e., a “hotspot”) to which the user device may connect. Upon receiving the address, the user device browser may navigate to the web page, which provides instructions for the user to bring an NFC-enabled smart card to within communication range of the user device. (This action may be referred to herein as “tapping” the transaction card to the user device.) The action of tapping the transaction card to the user device results in the transmission of NFC information from the transaction card through the user device to the smart apparatus via Web NFC at 1200.

[0027] The NFC information may be or include a unique identifier for the transaction card that is associated with a card account of the user. At 1300, the smart apparatus may transmit some or

all of the NFC information, including the card identifier, to the service administration server associated with the apparatus or a service to be provided by the apparatus. The apparatus may also transmit its own unique identifier. The service administration server may then use the NFC information to identify the administrator of the account associated with the card. At 1400, the service administration server transmits some or all of the NFC information, including the card identifier, to a server of the card account administrator. The card account administrator uses the NFC information to determine the account associated with the transaction card and transmits, at 1500, account information back to the service administration server. This account information may include information about the account holder that the service administration server can use to determine whether the user has an existing service account with the service administrator or to establish a new service account for the user. The service administration server may then associate the account information with the apparatus and transmit a service activation command to the apparatus at 1600. The service activation command may include default provisioning instructions or provisioning instructions determined based on existing service account preferences. In some embodiments, the service administration server may contact the user to prompt for and receive provisioning preferences.

[0028] From the user perspective, the above scenario provides a highly simplified activation/provisioning experience in which the user does no more than connect the apparatus, establish communication between the apparatus and the user device, open the web page identified by the apparatus, and tap the transaction card to the user device.

[0029] The systems and methods of the invention will now be discussed in more detail.

[0030] Figure 2 depicts a typical home-based smart apparatus control system 100 according to an embodiment of the invention that is usable in conjunction with the methods of the invention.

The smart apparatus control system 100 comprises a user processing device 110 and one or more smart appliances or other apparatus. As used herein, the term smart apparatus is used to refer to any controllable vehicle, appliance, or other mechanism or system that has a data processing system that can receive control instructions from a user data processing device (such as user device 110) either through direct wired or wireless communication or via a network (such as network 105). In the illustrative example of Figure 2, the smart apparatus of system 100 includes a vehicle 120, a refrigerator 130, a clothes washer 140, a heating and cooling system 150, a “smart speaker” 160, a Wi-Fi router 170, and a generic network-enabled apparatus 190. Each of these apparatus may be connected to one another via a local network 105 to which the user device 110 is also connected.

[0031] With reference to Figures 2 and 3, the generic smart apparatus 190 can be used to describe features that may be common to various smart apparatus usable in the systems of the invention. As shown in Figure 3, the smart apparatus 190 comprises a data processing system 191 and one or more mechanical and/or electrical operational systems 197. The operational system or systems 197 encompass all the operational hardware of the apparatus 190 that allow it to perform its function. In an appliance such as a refrigerator, for example, this would include all of the primary and secondary mechanisms and power supply systems for cooling the enclosed compartments. In a washer, it would include all of the mechanisms for filling, agitating, spinning and draining the wash drum. In a vehicle, it would include a variety of systems for powering, steering, braking, cooling, etc.

[0032] The data processing system 191 comprises the elements for communicating with the apparatus 190 and for controlling its operation. These may include a control data processor 192 configured for monitoring and controlling one or more operational parameters of the operational

system 197. Such parameters may be as simple as “on or off” or more complex such as the parameters associated with a wash cycle in a washer (e.g., control and timing of water filling and draining, water temperature, agitation cycling, etc.). Operational instructions for the control processor 192 may be stored in a memory module 195. These instructions may be a combination of permanently stored instructions and temporary, user-supplied instructions. In many instances, the memory 195 may have stored therein predetermined operational modes. The memory 195 may also have stored therein operational restrictions that prevent operation of the operational system 197 under predetermined circumstances (e.g., an over-heating condition or excessive current draw). These could require, for example, the control processor 192 to alter the operational mode of the operational system 197 or even shut it down completely.

[0033] The memory module 195 may also have stored therein one or more service applications comprising instructions for the apparatus data processing system to implement a service operation. These service applications may include instructions for the control processor 192 to implement operational instructions received from the user or from a service administrator associated with the apparatus 190 or with services provided by or through the apparatus 190. For example, in a case where the apparatus 190 is a router for use in connecting other devices to the Internet, the service administrator could be an ISP and one or more of the service applications may be established and/or controlled by the ISP.

[0034] The memory module 195 may have stored therein software for configuring a web page for facilitating initialization of apparatus 190 operation. The web page coding may include Web NFC JavaScript configured for reading transaction card-transmitted NFC information via the browser of a user device.

[0035] User input to the data processing system 191 may be received through the use of a user

interface 194, which may be or include any device for entering information, control input, and instructions into the system 191. In many cases, the user interface 194 may be a combination of buttons and/or dials having preset control functions. In some apparatus, the user interface 194 may include more complex devices such as a touch-screen, keyboard, mouse, cursor-control device, microphone, stylus, or digital camera.

[0036] The data processing system 191 also includes a local area communication interface 193 in communication with the control processor 192 and configured for communication over one or more networks such as the local network 105 of Figure 2. In particular, the communication interface 193 may be configured to allow the control processor 192 to transmit to and receive transmissions from the user device 110 via the local network 105. In some embodiments, the communication interface 193 may be configured to support short-range wireless communication (e.g., by NFC, radio-frequency identification (RFID), and/or Bluetooth). The data processing system 191 may also include a second communication interface 198 configured for connection to a wide area network (e.g., a telecommunications cable network) such as the network 230 of Figure 5. The wide area network communication interface may, in particular, be configured to transmit to and receive transmissions from one or more remote servers via a wide area network.

[0037] In some embodiments, the data processing system 191 may include a wireless hotspot module 199 in communication with the WAN communication interface 198. The hotspot module 199, in combination with software stored in the memory module 195, is configured for operation as a limited range wireless access point that may be accessed by the user device 110 for communication therewith.

[0038] The smart apparatus 190 may include a sensor arrangement 196 in communication with the control processor 192. The sensor arrangement 196 may be configured for monitoring one or

more operational parameters of the operational system 197 and/or a measurable parameter of the environment in which the apparatus 190 is operating. In the case of a refrigerator, for example, the sensor arrangement 196 could include temperature sensors for monitoring the temperature in various compartments of refrigerator. In a home heating system, the sensor arrangement 196 could include a room air temperature sensor. The sensor arrangement 196 may also include sensors for monitoring a condition or operating characteristic of the operational system 197. This could include, for example, a sensor for measuring an internal machine temperature that could, if it exceeds a certain level, result in damage to the apparatus. Sensor measurement information is transferred from the sensor arrangement 196 to the control processor 192, which uses it to control operation of the operational system 197.

[0039] The memory 195 may also have stored therein an apparatus activation application that may be configured for execution upon the apparatus first being powered up and connected to the Internet. The activation application may include instructions for the control processor 192 to receive, via the local network communication interface 193 or via the wireless hotspot module 199, a service initiation communication from a user device 110. The application may further include instructions to establish Internet communication via the wide area network communication interface 198 and to create a Web NFC-enabled web page. The application may then cause the control processor 192 to transmit to the user device via the local communication interface 193 or the wireless hotspot module 199, a communication that includes the address for the web page and instructs the user to navigate to the web page, which instructs the user to tap an NFC-enabled smart transaction card to the user device. The application then uses the Web NFC methodology to read NFC information transmitted to the user device by the smart transaction card, the NFC information including card identification information unique to the smart

transaction card. The application then causes the processor 192 to transmit the NFC information and to a service administration server along with an apparatus identifier stored in the memory 195. The application is configured to receive an activation command back from the service administration server. The service command may include initial operation instructions and/or initial provisioning options for configuring the apparatus for operation. In response, the application may activate apparatus operation and/or one or more service applications.

[0040] In some embodiments, the smart apparatus 190 may be a service apparatus configured for facilitating the delivery or monitoring of a utility (e.g., electricity, water, or gas service), a telecommunications link, or data delivery system (e.g., cable or satellite). In such embodiments, the service administrator may be the supplier of the utility, telecommunications service, or data delivery service. For example, if the smart apparatus is or is part of an electrical distribution system, the service administrator would be the power company supplying the electricity.

[0041] With reference to Figures 2 and 4, the account holder/user interface device 110 may be any data processing and/or communication device that an account holder uses to carry out a transaction and/or to receive notifications regarding an account including, but not limited to a smartphone, a laptop, a desktop computer, and a tablet. In particular embodiments, the account holder device 110 includes an on-board data processor 111 in communication with a memory module 113, a user interface 115, and a communication interface 117. The data processor 111 can include a microprocessor and associated processing circuitry, and can contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein. The memory 113 can be a

read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM and EEPROM, and the user device 110 can include one or more of these memories.

[0042] The user interface 115 includes a user input mechanism, which can be any device for entering information and instructions into the account holder device 110, such as a touch-screen, keyboard, mouse, cursor-control device, microphone, stylus, or digital camera. The user interface 115 may also include a display, which can be any type of device for presenting visual information such as a computer monitor, a flat panel display, and a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays.

[0043] The communication interface 117 is configured to establish and support wired or wireless data communication capability for connecting the device 110 to a broad network (e.g., network 230 of Figure 5), the local network 105, or other communication network. The communication interface 117 can also be configured to support communication with a short-range wireless communication interface, such as radio-frequency identification and Bluetooth. In particular, the communication interface 117 may be configured to detect and establish communication with the smart apparatus data processing system 191 via the wireless hotspot module 199.

[0044] The user device 110 may further include an NFC interface 119 that includes an NFC receiver configured for selectively activating a magnetic field for use in establishing near field communication with an NFC transmitter. The NFC interface 119 is configured for establishing NFC communication when a passive NFC tag or other NFC-enabled device is brought into the magnetic field and within NFC communication range of the user device 110. The NFC interface 119 is configured, in particular, for communication with an NFC-enabled smart transaction card 102 when the card 102 is tapped to the user device 110.

[0045] In embodiments of the invention, the memory 113 may have stored therein one or more applications usable by the data processor 111 to conduct and/or monitor transactions on a transaction account between the account holder device 110 and a merchant device or other device. These applications may include instructions usable by the data processor 111 to identify transaction events, store event data in the memory 113, and communicate event data to a transaction processing server and/or an account management server. Some applications may also include instructions relating to receiving and interpreting notifications and/or instructions from the transaction processor or account administration server (e.g., card account administration server 260 of Figure 5).

[0046] In particular embodiments, the memory 113 may have stored therein a financial monitoring application configured for receiving account information from an account management server. The account information may include information on any account parameter including, but not limited to, a current account balance, average account balance, project account balance, expenditures over a time interval or since a beginning date of a time interval (e.g., the first day of the month). The account information may also include information such as a previous account balance, information on recent transactions, information on projected or scheduled transactions (e.g., automatic deposits or withdrawals), and payments to particular merchants.

[0047] The user device memory 113 may also have stored therein a smart apparatus control application configured with instructions for the data processor 111 to construct and transmit control instructions to one or more of the smart apparatus 120, 130, 140, 150, 160, 170, 190 via the local network 105. The application may be configured to tailor these instructions according to information stored in the memory 113 for the apparatus being controlled. The instructions

associated with a generic apparatus 190 may include instructions for displaying prompts to the account holder for and receiving from the account holder via the user interface 115 control input information for the apparatus 190. The control input information may include an operation mode selection, specification of one or more operational parameters, and/or one or more desired apparatus output parameter. The control application may be configured to instruct the data processor to receive the control input information and construct apparatus control instructions and transmit them to the data processing system 191 of the apparatus 190 via the local network 105. The apparatus control instructions may include an instruction to set or change an operational parameter of the apparatus 190.

[0048] The control application may be further configured with instructions for receiving operation information from the data processing system 191 of the apparatus 190. The application may be configured to review this information and determine whether to display some or all of the information to the account holder via the user interface 115. In some embodiments, the control application may be configured to prompt for and receive additional control input information in response to the operation information received from the apparatus 190.

[0049] The user device memory 113 may also have stored therein an apparatus operation monitoring application having instructions configured for receiving information on the operation of an apparatus to determine if automated changes to its operation may be having a negative or unintended effect on the apparatus. This may include instructions to receive and evaluate operation information from any or all of the apparatus 120, 130, 140, 150, 160, 170, 190. Such operation information may include information on one or more measured operational parameters for the apparatus and/or measured environment parameters.

[0050] In some embodiments, the control application may include instructions for the data

processor 111 to use financial parameter information and operational parameter information along with empirical life expectancy and/or cost information for an apparatus 190 to determine an optimized set of operational parameters for that apparatus 190. The optimized set of operational parameters can then be included in change control instructions transmitted by the data processor 111 to the control processor 192 of the apparatus 190.

[0051] With reference now to Figure 5, a system 200 for activating a network-enabled smart apparatus 290 according to an embodiment of the invention may include a user device 210, which may be in selective communication with the smart apparatus 290 via a local network 205. The user device 210 and local network 205 may be similar to those previously described in relation to the apparatus control system 100. The system 200 may also include an Internet service provider 240, an apparatus service administration server 250, and a card account administration server 260, all of which may be in contact with one another or with the user device 210 and/or the smart apparatus 290 via a wide area network 230.

[0052] The various components of the system 200 may include various network-enabled computer systems configured for processing information and transactions involving a plurality of service accounts administered by an apparatus service administrator and/or a plurality of transaction card accounts administered by a financial institution, merchant or other card account administrator. As referred to herein, a network-enabled computer system and/or device may include, but is not limited to any computer device, or communications device including, a server, a microprocessor or system of microprocessors, a network appliance, a personal computer (PC), a workstation, and a mobile processing device such as a smart phone, smart pad, handheld PC, or personal digital assistant (PDA). In some examples, the computer device may use instructions stored on a computer-accessible medium (e.g., a storage device such as a hard disk, floppy disk,

memory stick, CD-ROM, RAM, ROM, etc., or a collection thereof). The computer-accessible medium can contain executable instructions thereon. In addition or alternatively, a storage arrangement can be provided separately from the computer-accessible medium, which can provide the instructions to the processing arrangement so as to configure the processing arrangement to execute certain exemplary procedures, processes, and methods, as described herein.

[0053] The network-enabled computer systems used to carry out the actions contemplated by the invention may execute one or more software applications to, for example, receive data as input from an entity accessing the network-enabled computer system, process received data, transmit data over a network, and receive data over a network. The one or more network-enabled computer systems may also include one or more software applications to notify an account holder based on transaction information.

[0054] It will be understood that the depiction in Figure 5 is an example only, and the functions and processes described herein may be performed by any number of network-enabled computers. It will also be understood that where the illustrated system 200 may have only a single instance of certain components, multiple instances of these components may be used. The system 200 may also include other devices not depicted in Figure 5.

[0055] The network 230 may be any form of communication network capable of enabling communication between the subsystems of the system 200. For example, the network 230 may be one or more of a wireless network, a wired network or any combination of wireless network and wired network. The network 230 may be or include one or more of a fiber optics network, a passive optical network, a cable network, an Internet network, a satellite network, a wireless LAN, a Global System for Mobile Communication (“GSM”), a Personal Communication Service

(“PCS”), a Personal Area Network (“PAN”), Wireless Application Protocol (WAP), Multimedia Messaging Service (MMS), Enhanced Messaging Service (EMS), Short Message Service (SMS), Time Division Multiplexing (TDM) based systems, Code Division Multiple Access (CDMA) based systems, D-AMPS, Wi-Fi, Fixed Wireless Data, IEEE 802.11b, 802.15.1, 802.11n and 802.11g or any other wired or wireless network for transmitting and receiving a data signal. The network 230 may utilize one or more protocols of one or more network elements to which it is communicatively coupled. The network 230 may translate to or from other protocols to one or more protocols of network devices. Although the network 230 is depicted as a single network, it will be appreciated that it may comprise a plurality of interconnected networks, such as, for example, the Internet, a service provider’s network, a cable television network, corporate networks, and home networks.

[0056] In the example embodiments presented herein, an account holder may be any individual or entity permitted to conduct a transaction (which may be, but is not limited to a financial transaction) using a transaction card account. An account may be held by any place, location, object, entity, or other mechanism for holding money or performing transactions in any form, including, without limitation, electronic form. An account may be, for example, a credit card account, a prepaid card account, stored value card account, debit card account, check card account, payroll card account, gift card account, prepaid credit card account, charge card account, checking account, rewards account, line of credit account, credit account, mobile device account, or mobile commerce account. An account holder may be a transaction processing entity such as a financial institution, credit card provider, or other entity that offers accounts to customers.

[0057] A transaction account may be associated with one or more smart transaction cards 220

(e.g., debit cards, credit cards, or prepaid account cards). Alternatively or in addition, the transaction account may be associated with one or more account holder processing devices or simply associated with a unique identifier enterable by an account holder to facilitate a transaction. The processing devices may be configured to act as a method of payment at a POS location using, for example, NFC or any other mobile payment technology. In some embodiments, separate cards or user devices may be associated with individual account co-holders.

[0058] The transaction card 220 may be any chip-carrying transaction card (“smart” card) having electrical and/or near field or other short range communication capabilities. As illustrated in Figures 5 and 6, a typical transaction card 220 that is usable in various embodiments of the invention is a smart card with a microprocessor chip 221. The microprocessor chip 221 includes processing circuitry for storing and processing information, including a microprocessor 222 and a memory 226. It will be understood that the processing circuitry may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein.

[0059] The transaction card 220 is configured for communication with transaction terminals and other device via a first communication interface 224. The interface 224 and the microprocessor 222 may, in particular, be configured for establishing communication with merchant transaction processing devices for carrying out purchase and other transactions. The communication interface 224 may be configured to provide for contact-based communication, in which case the interface 224 may have electrical circuitry and contact pads on the surface of the card 220 for establishing direct electrical communication between the microprocessor 222 and the processing

circuitry of a transaction terminal. Alternatively or in addition, the first communication interface 224 may be configured for contactless communication with a transaction terminal or other wireless device. In such embodiments, the communication interface 224 may be or include an NFC communication interface configured for communication with other NFC communication devices when the card 220 is within a predetermined NFC range. The communication interface 224 and the microprocessor 222 may, in particular, be configured for establishing NFC communication with the user device 210. In some embodiments, the microprocessor chip 221 may include a second communication interface 228 configured for establishing short range communication with the user device 210 via Bluetooth, or other short range communication methodology. In such embodiments, the transaction card 220 may have a short range communication antenna 229 that is included in or connected to the short range communication interface 228. The microprocessor chip 221 may also include a power management system 225 for use in managing the distribution of power during an NFC transaction.

[0060] In particular embodiments, the transaction card 220 may be Bluetooth enabled using the microprocessor chip 221, the second communication interface 228 and the antenna 229. A Bluetooth-enabled transaction card may support Bluetooth Low Energy (BLE) and may be paired to the user device 210. In some embodiments, pairing and communications may be established between the transaction card 220 and other interfacing devices, such as a terminal (not shown), a merchant transaction processor 140, and the like. A Bluetooth-enabled device may include the capabilities to establish a link between a card and the device (or pair the devices) using device settings (e.g., iOS or Android settings that manage Bluetooth connections) and/or mobile application(s) associated with the card issuer that can cooperate with the device controls to manage a Bluetooth connection with the card 220.

[0061] The memory 226 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the chip 221 may include one or more of these memories. The memory 226 may have stored therein information associated with a transaction card account. In some embodiments, the memory 226 may have permanently stored therein a unique alphanumeric identifier associated with the account. It may also have stored public and private card encryption keys. In some embodiments, the private and public encryption keys may be permanently hard-wired into the card memory.

[0062] The memory 226 may be configured to store one or more software applications for execution by the microprocessor 222. In various embodiments, the memory 226 may have stored therein instructions for generating encrypted information and transmitting it to a receiving device (e.g., the user device 210) via the first communication interface 224 (e.g., via NFC) or the short-range communication interface 228. Such encrypted information may be or include an encrypted verification block or signature that may be used to authenticate and verify the presence of the transaction card 220 during transaction processing. In some embodiments, encrypted information be unique to a particular communication (e.g., a particular NFC transmission by the transaction card).

[0063] The apparatus service administration server 250 may be associated with and/or managed by the manufacturer or the seller (or lessor) of the smart apparatus 290. Alternatively, the service administration server 250 may be associated with a provider of a service administered through the apparatus 290. With reference to Figure 7, the apparatus service administration server 250 may include a communication interface 252 providing a wired and/or wireless connection to the network 230, an apparatus initialization processor 254 and a service account management processor 256. The apparatus initialization processor 254 is configured to receive

an initialization request from the apparatus 290, the request including some or all of the NFC information read from the transaction card 220 and identification information for the apparatus 290. The apparatus initialization processor 254 may be further configured to use the NFC information to identify a card account administrator associated with the transaction card 220 and to transmit a card account information request to the card account administration server 260 of the card account administrator. This request may include some or all of the NFC information, including card identification information, some or all of which may be encrypted. The apparatus initialization processor 254 is also configured to receive card account information back from the card account administration server 260. Such information may include identification, contact, and other information relating to the account holder. This information may be forwarded by the initialization processor 254 to the service account management processor 256.

[0064] The service account management processor 256 in communication with account information database 251 is configured to receive card account holder information from the apparatus initialization processor 254. The service account management processor 256 may then use the card account holder information to identify the card user and determine whether the user has a service account with the service provider. This may be accomplished by comparing the card account information with account information stored in a service account information database 251. If the user has an account, the processor 256 may associate the apparatus identifier of the apparatus 290 with the existing service account of the user. If the user does not have an existing account, the processor 256 may create a new service account using the card account information for the user. In some embodiments, the service account management processor 256 may contact the user (e.g., via a transmission to the user device 210 over the network 230) to verify that the user wishes to open a new service account or to obtain user preferences in

establishing the account and/or operational parameters of the smart apparatus 290. The service account management processor 256 may then associate the smart apparatus 290 with the new account and store the service account information in the account information database 251.

[0065] Upon associating the apparatus 290 with either an existing account or a new account, the account management processor 256 may then send the service account information back to the initialization processor 254, which constructs and transmits an initialization command to the smart apparatus 290. This command may include initial provisioning information as well as an instruction to initiate apparatus operation.

[0066] In some embodiments, the service administration server 250 may also include an apparatus operation management processor 258, which is configured to communicate with the apparatus 290 for monitoring and management of apparatus operation. In some cases, the operation management processor 258 may communicate with the user regarding the user's operational preferences or instructions. The apparatus operation management processor 258 may also be configured to provide system updates to the data processing system of the smart apparatus 290. In some embodiments, the operation management processor 258 may also be configured to determine time or use-based service fees associated with the use of the apparatus or for services accessed or used via the apparatus. The operation management processor 258 may also be configured to automatically charge some or all of such service fees to the transaction card account associated with the transaction card 220 or to another financial account of the service account holder.

[0067] The card account administration server 260 is a system of one or more network-enabled processing servers configured to monitor and/or process transactions involving the transaction card 220 and to process information requests relating to a card account associated with the

transaction card 220. With reference to Figure 8, the card account administration server 260 includes a transaction communication interface 262 that is connected to the network 230 for communication with the user device 210 and merchant devices.

[0068] The card account administration server 260 has a transaction processor 264 and a card account information server 266, both of which are configured for communication over the network 230 via the transaction communication interface 262. The card account information server 266 may be configured for maintaining a transaction card account database (not shown) in which is stored identification information for each of the plurality of transferable cards along with associated account information. Such account information may include identification, contact, and other information relating to the account holder.

[0069] The card account information server 266 may be further configured for assigning private and public personal encryption keys to an account of an account holder to whom a transaction card 220 has been issued or is to be issued. Once assigned, the card management server may transmit, via the network 230, the personal encryption keys to a user device 210 associated with the account holder. The card processing system may be further configured to receive a request from the user device 210, via the network 230 and the transaction communication interface 262, to activate the transaction card 220. The activation request includes a software signature encrypted by the user device 210 using the public and private personal encryption keys and a hardware signature encrypted by of the card's microprocessor chip 221 using the public and private card encryption keys stored therein. The card account information server 266 is further configured to, upon receiving the activation request, decrypt the software and hardware signatures to verify their association with the account, and, upon positive verification, activate the transaction card 220 by associating one or more authorized account functions with the

transaction card 220. The server 266 may then store information reflecting the activation in the card database. An authorized account function could be any typical transaction card functionality such as, for example, interaction with a merchant transaction processing device to carry out a purchase transaction or use in an automatic teller machine. In particular embodiments, the authorized account functions may include the use of the transaction card 220 to initiate service and/or create a service account associated with the smart apparatus 290.

[0070] The card account information server 266 may also be configured to receive account information requests from a merchant or service account administrator to whom the transaction card 220 has been presented. In particular, the server 266 may be configured to receive an account information request from the service account management processor 256. The request may include NFC information transmitted by the transaction card 220 and read by the smart apparatus 290. In embodiments where a portion of the NFC information is encrypted using keys stored on the transaction card, the server 266 may be configured to retrieve the encryption keys associated with the transaction card 220 and decrypt the encrypted information to authenticate the and verify the presence of the transaction card 220.

[0071] Figure 9 is a diagram of a method M100 of activating a network-enabled smart apparatus according to an embodiment of the invention. The method involves the use of an NFC-enabled user device and an NFC-enabled smart transaction card to activate the smart apparatus, which may be any appliance, vehicle or system having attributes similar to those of the generic apparatus 190 of Figure 3. Some or all of the actions of method M100 may be carried out by the data processing system of the smart apparatus being activated. The method M100 includes, at S110, establishing an Internet connection by the apparatus data processing system. This may be carried out through a wired or wireless connection to an ISP or through a connection to a

telecommunications network. In some embodiments, this action may be taken immediately upon the apparatus being powered up by the user for the first time. At S120, the data processing system of the smart apparatus creates a web page configured for use in conducting a Web NFC read of information from the transaction card. At S130, the apparatus data processing system transmits the webpage location to the user device. This may be accomplished via a connection of the smart apparatus to a local network. Alternatively, if so configured, the smart apparatus may transmit the information via a self-generated hotspot to which the user device has connected. In either case, the transmission may be in response to establishment of communication by the user device and upon receiving a request to initiate operation. In some embodiments, such communication between the user device and the apparatus may be established prior to the apparatus establishing the Internet connection. In such embodiments, the establishment of the Internet connection may be triggered by the establishment of communication with the user device or the receipt of an initiation request.

[0072] At S140, the apparatus data processing system transmits an instruction to the user device to tap the transaction card to the user device. This instruction may be presented via the web page or by a separate transmission via the local network or apparatus-generated hotspot. Upon the user tapping the transaction card to the user device, the apparatus data processing system reads, via Web NFC code, NFC information transmitted to the user device by the transaction card at S150. The NFC information includes, at least, sufficient information to identify the transaction card administrator and information usable by the transaction card administrator to identify the card and its associated transaction account. At S160, the apparatus data processing system transmits an activation request to the service administration server via the apparatus's network connection. The activation request may include a unique identifier for the apparatus and some or

all of the NFC information read from the transaction card. At S170, the apparatus data processing system receives a service activation command from the service administration server. This command may include an instruction to initiate operation and/or initial operation and provisioning instructions. In some embodiments, the apparatus may also receive service account information. At S180, the apparatus initiates operation or, in some cases, established operational readiness. In the latter cases, the apparatus may require additional instruction or manipulation by the user before actually “turning on”. In some embodiments, the apparatus may optionally send a service initiation notification to the user device at S190. This may be transmitted via the local network, the apparatus’s self-generated hotspot, or through the wide area or other communications network.

[0073] Figure 10 is a diagram of a method M200 of activating a network-enabled smart apparatus according to an embodiment of the invention. Some or all of the actions of method M200 may be carried out by an apparatus service administration server managed by an administrator having an association with the smart apparatus being activated or a service to be provided via the smart apparatus being activated. At S210 of the method M200, the administration server receives an activation request from the smart apparatus via a network. The activation request includes identification information unique to the smart apparatus. The request may also include NFC information read by the smart apparatus from a smart transaction card, the NFC information having been transmitted by the transaction card to a user device of a holder of a card account associated with the transaction card.

[0074] At S220, the service administration server uses the NFC information to identify a card account administrator associated with the transaction card transmits a card account information request to a card account administration server of that administrator. This request may include

some or all of the NFC information, including card identification information, some or all of which may be encrypted. At S230, the service administration server receives card account information back from the card account administration server. This information may include identification, contact, and other information relating to the account holder/user. At S240, the server uses the account information to identify the account holder/user wishing to activate the smart apparatus. At S250, the server associates the apparatus identification information with a service account associated with the account holder. The account and apparatus ID information may be stored by the server in a service account information database. At S260, the service administration server may optionally determine user preferences for apparatus service or operating parameters. If the account holder already had an existing account, this may include importing previously established preferences for the account holder. Alternatively or in addition, the account holder may be contacted to provide or confirm the account holder's preferences. At S270, the server constructs a service activation command. This command may include an instruction to initiate operation and/or initial operation and provisioning instructions, which may be based on user preferences. In some embodiments, the command may also include service account and/or account holder information. At S280, the service administration server transmits the service activation command to the smart apparatus via the network.

[0075] Figure 11 is a diagram of a method M300 of activating a network-enabled smart apparatus according to an embodiment of the invention. Some or all of the actions of method M300 may be carried out by an apparatus service administration server managed by an administrator having an association with the smart apparatus being activated or a service to be provided via the smart apparatus being activated. At S310 of the method M200, the administration server receives an activation request from the smart apparatus via a network. The

activation request includes identification information unique to the smart apparatus. The request may also include NFC information read by the smart apparatus from a smart transaction card, the NFC information having been transmitted by the transaction card to a user device of a holder of a card account associated with the transaction card.

[0076] At S320, the service administration server uses the NFC information to identify a card account administrator associated with the transaction card and, at S330, transmits a card account information request to a card account administration server of that administrator. This request may include some or all of the NFC information, including card identification information, some or all of which may be encrypted. At S340, the service administration server receives card account information back from the card account administration server. This information may include identification, contact, and other information relating to the account holder/user. At S350, the server uses the account information to identify the card account holder wishing to activate the smart apparatus and determines whether that card account holder has a service account with the service administrator. This may include comparing the card account information with account information stored in a service account information database. If the user has an account, the processor sets the current service account to be the existing account at S351. If the user does not have an existing account, the server may create a new service account at S352 using the card account information. In some embodiments, the service administration server may contact the card account holder (e.g., via a transmission to the account holder's user device over the network) to verify that the user wishes to open a new service account or to obtain user preferences in establishing the account and/or operational parameters of the smart apparatus. After opening the new account, the service administration server may then set the current account to be the new service account at S354. At S360, the server may associate the smart

apparatus with the existing or new account as appropriate and store the service account information in the account information database.

[0077] At S370, the service administration server may optionally determine user preferences for apparatus service or operating parameters. If the account holder already had an existing account, this may include importing previously established preferences for the account holder.

Alternatively or in addition, the account holder may be contacted to provide or confirm the account holder's preferences. At S380, the server constructs a service activation command. This command may include an instruction to initiate operation and/or initial operation and provisioning instructions, which may be based on user preferences. In some embodiments, the command may also include service account and/or account holder information. At S390, the service administration server transmits the service activation command to the smart apparatus via the network.

[0078] The present invention provides a significant improvement in the security and efficiency of systems initiating operation of smart appliances, vehicles, and other apparatus by eliminating the need to download a specialized application to a user device. The method also enhances security by providing direct pass-through of transaction card identification information without interpretation or decryption by the user device being used to activate the apparatus.

It will be readily understood by those persons skilled in the art that the present invention is susceptible to broad utility and application. Many embodiments and adaptations of the present invention other than those herein described, as well as many variations, modifications and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and foregoing description thereof, without departing from the substance or scope of the invention.

CLAIMS

What is claimed is:

1. A network-enabled apparatus comprising:

- an apparatus data processing system;
- at least one operational system in communication with the apparatus data processing system and configured for carrying out a mechanical or electrical operation;
- a first network communication interface configured for establishing communication over a wide area network;
- a second network communication interface configured for establishing communication over a local network; and
- a memory having stored therein apparatus identification information, at least one service application comprising instructions for the apparatus data processing system to implement a service operation using the at least one operational system, and an activation application comprising instructions for the apparatus data processing system to
 - establish an internet connection via the first network communication interface,
 - create a near field communication (NFC)-enabled web page,
 - transmit, to a user device via the second communication interface, an instruction to navigate to the NFC-enabled web page,
 - transmit to the user device via the NFC-enabled web page an instruction for a user of the user device to tap an NFC-enabled smart transaction card to the user device,
 - read, via the NFC-enabled web page, NFC information transmitted to the user

device by the smart transaction card, the NFC information including card identification information unique to the smart transaction card, transmit the NFC information and the apparatus identification information to a service administration server, receive, from the service administration server, a service activation command, and responsive to the service activation command, activate at least one of the at least one service application.

2. A network-enabled apparatus according to claim 1 wherein the second network communication interface comprises a wireless access point module configured for operation as a wireless local area network communication node, the activation application further comprises instructions for the apparatus data processing system to activate the wireless local area network communication node, and a service initiation communication is received from the user device via the wireless local area network node.
3. A network-enabled apparatus according to claim 1 wherein the activation application further comprises instructions for the apparatus data processing system to establish a connection to a local area network, and a service initiation communication is received from the user device via the local area network.
4. A network-enabled apparatus according to claim 1 wherein the service administrator is an internet service provider and the apparatus comprises a network router.

5. A network-enabled apparatus according to claim 1 wherein the apparatus is or includes a household appliance.
6. A network-enabled apparatus according to claim 1 wherein the apparatus is or includes an electrical distribution system.
7. A network-enabled apparatus according to claim 1 wherein the apparatus is or includes a household environmental control system.
8. A method for activating a network-enabled apparatus using a near field communication (NFC)-enabled user device and an NFC-enabled smart transaction card associated with a card account, the method comprising:
 - establishing an internet connection by the network-enabled apparatus;
 - creating an NFC-enabled web page by the network-enabled apparatus;
 - transmitting, by the network-enabled apparatus to the user device, an instruction to
 - navigate to the NFC-enabled web page;
 - transmitting, by the network-enabled apparatus to the user device via the NFC-enabled web page, an instruction for the user to tap the smart transaction card to the user device;
 - reading, by the network-enabled apparatus via the NFC-enabled web page, NFC information transmitted to the user device by the smart transaction card, the NFC information including card identification information unique to the smart transaction card;
 - transmitting, by the network-enabled apparatus to a service administration server of a service administrator, the NFC information and apparatus identification information;

identifying, by the service administration server using the apparatus identification information, the network-enabled apparatus;
transmitting the NFC information by the service administration server to a card administration server;
receiving, by the service administration server from the card administration server, card account information associated with the card account;
identifying an account holder by the service administration server using the card account information;
associating, by the service administration server, the network-enabled apparatus with the card account and an apparatus service account with the service administrator; and
transmitting, by the service administration server to the network-enabled apparatus, a service activation command.

9. A method according to claim 8 further comprising:

establishing a connection between the network-enabled apparatus and a wide area network; and
activating, by the network-enabled apparatus, a wireless local area network node for communication with the user device,
wherein a service initiation communication is received from the user device via the wireless local area network node, and
wherein the internet connection is established via the wide area network.

10. A method according to claim 8 further comprising:

receiving a service initiation communication by the network-enabled apparatus from the user device.

11. A method according to claim 8 wherein at least a portion of the NFC information is encrypted information.
12. A method according to claim 11 wherein the encrypted information was encrypted by the smart transaction card and includes information unique to the NFC transmission by the transaction card to the user device.
13. A method according to claim 8 wherein the card account information includes identification of a card account holder associated with the smart transaction card.
14. A method according to claim 13 further comprising:
 - determining, by the service administration server, whether the card account holder has an existing service administrator account; and
 - responsive to a determination that the card account holder has an existing service administrator account, setting the apparatus service account to be the existing service administrator account.
15. A method according to claim 14 further comprising:
 - responsive to a determination that the card account holder does not have an existing service administrator account,
 - establishing a new service administrator account for the card account holder using the card account information, and
 - setting the apparatus service account to be the new service administrator account.
16. A method according to claim 8 further comprising:
 - establishing a connection between the network-enabled apparatus and a wide area network; and

establishing a connection between the network-enabled apparatus and a local area network,
wherein a service initiation communication is received from the user device via the local area network, and
wherein the internet connection is established via the wide area network.

17. A method for activating a network-enabled apparatus using a near field communication (NFC)-enabled user device and an NFC-enabled smart transaction card associated with a card account, the method comprising:

establishing communication between the network-enabled apparatus and the user device;
creating an NFC-enabled web page by the network-enabled apparatus;
navigating to the NFC-enabled webpage by a web browser on the user device;
establishing NFC communication between the smart transaction card and the user device;
reading, by the network-enabled apparatus via the NFC-enabled web page, NFC information transmitted to the user device by the smart transaction card, the NFC information including card identification information unique to the smart transaction card;
transmitting, by the network-enabled apparatus to a service administration server, the NFC information and apparatus identification information;
transmitting the NFC information by the service administration server to a card administration server;
identifying, by the card administration server using the NFC information, a card account associated with the smart transaction card;
transmitting, by the card administration server to the service administration server, card

account information associated with the card account;
identifying an account holder by the service administration server using the card account information;
associating, by the service administration server, the network-enabled apparatus with the card account and an apparatus service account with the service administrator; and
transmitting, by the service administration server to the network-enabled apparatus from the service administration server, a service activation command.

18. A method according to claim 17 wherein at least a portion of the NFC information is encrypted information.

19. A method according to claim 18 wherein the encrypted information was encrypted by the smart transaction card and includes information unique to the NFC transmission to the user device.

20. A method according to claim 18 further comprising:

authenticating the smart transaction card by the card administration server,
wherein the action of authenticating includes decrypting the encrypted information.